اُردو زَبان میں اِنفارمیشن ٹیکنالوجی کا واحِد مُستند جریدہ

نومبر 2015

قیمت 65 روپے

پاکستان پوسٹ رجسٹریشن نمبر MC-1264

ماہنامہ کمپیوٹنگ

CompTIA Linux+
vmware CERTIFIED
CISCO CERTIFIED CCNA
CompTIA A+ CERTIFIED
CISCO CERTIFIED CCIE ROUTING AND SWITCHING
CompTIA Security+
Microsoft CERTIFIED Systems Engineer
Network+ CERTIFIED
CompTIA ADVANCED SECURITY PRACTITIONER CASP
Microsoft CERTIFIED Solutions Master
Microsoft CERTIFIED Application Developer
CISSP
CISCO CERTIFIED CCNP

نقل کے شاطر ذہنوں اور آئی ٹی سرٹیفکیشنز کے نگراں اداروں کی دلچسپ رسّہ کشی

فیس بک کی پندرہ حیران کن باتیں

مائیکروسافٹ آفس 2016 کے نئے فیچرز

کمپیوٹنگ ٹپس
دلچسپ اور مفید ٹوٹکے

سوشل میڈیا ہیکرز کی جنت

فہرست

مستقل سلسلے

جلد نمبر 9......شمارہ نمبر 07......نومبر 2015ء

سرپرستِ اعلیٰ

گوہر رحمان

مدیر اعلیٰ

امانت علی گوہر

مدیر

علمدار حسین

نائب مدیر

رانا محمد امین اکبر

مجلسِ مشاورت

شبیر حسین قریشی، محبوب الٰہی مخمور

قیمت فی شمارہ

65 روپے

زرسالانہ برائے پاکستان (رجسٹرڈ ڈاک)

850 روپے سالانہ

خط و کتابت کا پتا

پی او باکس نمبر 786، کراچی 74200

ٹیلی فون نمبر

0342 2507 857

دفتری اوقات

صبح 10 بجے تا سہ پہر چار بجے

ای میل ایڈریس

crm@computingpk.com

پوسٹل رجسٹریشن

MC-1264

ایک نئی تکنیک جس کے ذریعے اسمارٹ فون پر امیج پروسیسنگ آسان ہوگئی



آج کل کے دور میں اسمارٹ فون ہی لوگوں کے کمپیوٹر اور کیمرہ کی ضرورت کو پورا کر رہے ہیں۔ ایسے میں امیج پراسیسنگ ایپلی کیشنز کے موبائل ورژن کی طلب میں کافی اضافہ ہو رہا ہے۔ امیج پراسیسنگ ایک پیچیدہ کام ہے اور اس کے دوران ڈیوائس اپنی مکمل کمپیوٹنگ پاور استعمال کرتی ہے۔ جس کا نتیجہ بیٹری کے جلد ختم ہونے کی صورت میں نکلتا ہے۔ کچھ موبائل ایپلی کیشنز نے اس مسئلے کا حل اس طرح نکالا ہے کہ وہ تصویر کو اپنے کلاؤڈ سرور پر منتقل کرتی ہیں اور پراسیس کرنے کے بعد واپس صارف کو بھیج دیتی ہیں۔ لیکن اس سے ایک اور مسئلہ بھی پیدا ہو گیا۔ بڑے سائز کی فائل کو سرور پر منتقل کرنے اور واپس صارف کو بھیجنے سے جہاں پراسس تاخیر کا شکار ہونے لگا وہیں صارف کو بینڈ وڈتھ کے زیادہ استعمال سے اضافی خرچہ بھی برداشت کرنا پڑا۔

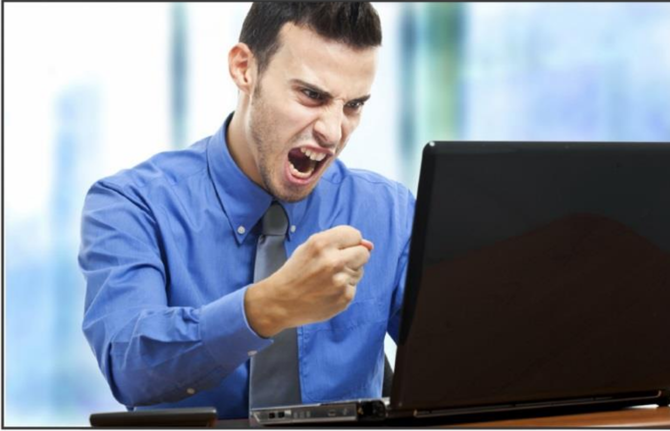
حال ہی میں ہونے والی سگ گراف (Siggraph) ایشیاء کانفرنس میں ایم آئی ٹی، اسٹینفورڈ یونیورسٹی اور ایڈوبی سسٹمز نے ایک حل پیش کیا۔ اس نئے حل یا نظام کی بدولت سرور پر کی جانے والی امیج پراسیسنگ کی وجہ سے خرچ ہونے والی بینڈ وڈتھ میں 98.5 فیصد تک کی زبردست کمی کی جاسکتی ہے۔ یہی نہیں، ڈیوائس کی 85 فیصد تک کمپیوٹنگ پاور بھی بچائی جاسکتی ہے۔

یہ سسٹم سرور کو تصویر کا انتہائی کمپریس ورژن بھیجتا ہے اور سرور جواب میں تمام پروسیسنگ کے بعد ایک چھوٹی سی فائل بھیجتا ہے۔ اس فائل میں صرف وہ ہدایات درج ہوتی ہیں جن کی تحت سسٹم کو اصل تصویر میں تبدیلی کرنا ہوتی ہے۔ یعنی جواب میں مکمل ترمیم شدہ تصویر بھیجنے کے بجائے اصل تصویر میں ترامیم کرنے کی ہدایات بھیج دی جاتی ہیں۔ مائیکل گھاربی، جو ایم آئی ٹی کے الیکٹریکل انجینیئرنگ اینڈ کمپیوٹر سائنس کے گریجویٹ اسٹوڈنٹ ہیں، نے بتایا کہ جیسے جیسے امیج پراسیسنگ کا الگورتھم بہتر ہوتا جائے گا، یہ تکنیک زیادہ مفید ہوجائے گی۔ انہوں نے کہا کہ ہم نت نئے الگورتھم دیکھ رہے ہیں جو بڑے ڈیٹا بیسز کا فائدہ اٹھاتے ہوئے پکسل کی سطح پر فیصلہ کرنے کی صلاحیت رکھتے ہیں۔

ابھی چونکہ یہ نظام اپنے ابتدائی مراحل میں ہے، اس لئے اس نظام کی صلاحیتیں محدود ہیں۔ فی الوقت یہ نظام صرف تصویر کے اسٹائل میں تبدیلی کرسکتا ہے جیسا کہ معروف سروس انسٹاگرام کے فلٹر تصویر کے اسٹائل تبدیل کرتے ہیں۔ تصویر میں ایسی تبدیلیاں جو کہ تصویر میں موجود اجسام یا مواد کی خدوخال ہی بدل رہی ہوں، اس نظام کے ذریعے نہیں کی جاسکتیں۔ قصہ مختصر کہ یہ نظام فوٹو شاپ جیسی تدوین کرنے کے قابل نہیں۔

تفصیلات کے مطابق بینڈ وڈتھ بچانے کے لئے یہ سسٹم سرور پر کم ریزولوشن کی JPG فارمیٹ کی تصویر اپ لوڈ کرتا ہے۔ پھر تصویر پر ہونے والی ہر کاروائی سرور انجام دیتا ہے۔ کم ریزلوشن تصویر کی وجہ سے بینڈ وڈتھ تو بچ جاتی ہے لیکن سرور کے لئے تصویر کی تدوین ایک مشکل کام بن جاتی ہے۔ تاہم ذہین الگورتھم کے استعمال سے اس مسئلے پر بھی قابو پالیا گیا۔ سرور جب پروسیسنگ کے بعد ہدایات پر مبنی فائل واپس بھیجتا ہے تو ڈیوائس جو کہ اسمارٹ فون یا کوئی ٹیبلٹ ہوسکتا ہے، کو ہدایات پر عمل کرنے کے لئے کچھ کمپیوٹنگ پاور خرچ کرنی پڑتی ہے۔ تاہم یہ فائل کو اپ لوڈ کرنے پر خرچ ہونے والی کمپیوٹنگ پاور سے بھی کم ہوتی ہے۔

آپ کو اگر آتا ہے غصہ زیادہ، تو شاید آپ کرتے ہیں فیس بک کا استعمال زیادہ



فیس بک اور سوشل میڈیا نے ہماری ذہنی صحت پر گہرا اثر ڈالا ہے۔ اس حوالے سے ماہنامہ کمپیوٹنگ کے انہی صفحات پر درجنوں خبریں پہلے بھی شائع ہو چکی ہیں۔ اب ایک تازہ ترین تحقیق کے مطابق فیس بک لوگوں کو تنہا اور غصیلا بنا رہا ہے۔ اس کی وجہ یہ ہے کہ لوگ مسلسل اپنا موازنہ دوسروں سے کرتے رہتے ہیں۔ یعنی اگلی بار جب آپ سے کوئی کہے کہ بھئی تم تو بہت غصہ کرنے لگے ہو، تو آپ سوشل میڈیا استعمال کرنے کی اپنی عادتوں پر بھی غور کیجئے گا۔

اس نئی تحقیق سے پتا چلا ہے کہ فیس بک کے لائکس اور دوستی کی درخواستیں صارفین کو فوری مگر عارضی خوشی فراہم کرتے ہیں لیکن یہی چیز ایک مصنوعی تاثر کو جنم دیتی ہے جو دوسرے صارفین کی بے اطمینانی کا باعث بنتی ہے۔ فیس بک صارفین سمجھتے ہیں کہ دوسرے لوگ اُن سے زیادہ خوش ہیں۔ کسی فیس بک صارف کو اچھا کھاتا، اچھا پہنتا اور اچھی جگہوں پر سیر کے لئے جاتا دیکھ کر دوسرے فیس بک صارفین کو محسوس ہوتا ہے کہ ان کی زندگی میں چونکہ یہ سب کچھ نہیں ہے، اس لئے وہ ان سے کم اچھی زندگی گزار رہے ہیں۔

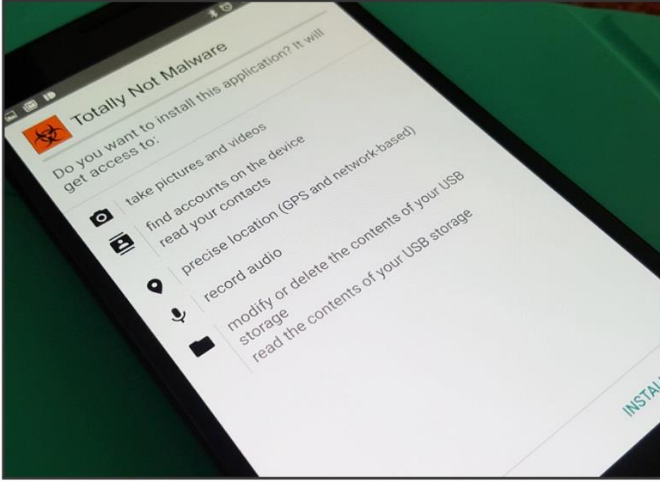
ڈنمارک کے ہیپی نیس ریسرچ انسٹی ٹیوٹ نے ایک تجربہ کیا۔ اس تجربے میں ڈنمارک کے 1095 افراد شریک ہوئے۔ ان تمام افراد سے اپنی خوشی کا لیول بیان کرنے کا کہا۔ لوگوں نے اپنی خوشی کو اوسطاً 10 میں سے 7.6 نمبر دیئے۔ اس کے بعد ان تمام افراد میں سے آدھے افراد کو کہا گیا کہ وہ ایک ہفتے کے لیے فیس بک کا استعمال کرنا بند کر دیں جبکہ دوسرے افراد کو فیس بک کا استعمال جاری رکھنے کا کہا گیا۔ 7 دنوں کے بعد اُن افراد سے دوبارہ اپنی خوشی کا لیول بیان کرنے کو کہا گیا جنہوں نے فیس بک استعمال نہیں کیا تھا تو اُن لوگوں نے اپنی خوشی کا لیول 8.12 بتایا جبکہ وہ افراد جو فیس بک استعمال کرتے رہے ان کا خوشی کا لیول پہلے جتنا ہی رہا۔ ایسے افراد جنہوں نے ایک ہفتے تک فیس بک استعمال نہیں کیا تھا، انہوں نے بتایا کہ اس دوران اُن کی حقیقی زندگی کی سماجی سرگرمیوں میں بھی اضافہ ہوا ہے۔ انہوں نے یہ بھی بتایا کہ فیس بک استعمال نہ کرنے کے دوران وہ کم غصے میں رہے اور خود کو فیس پہلے کے مقابلے میں کم تنہا محسوس کیا۔

ہیپی نیس ریسرچ انسٹی ٹیوٹ کے سی ای او میک وائیکنگ نے بتایا کہ تجربات کے ان نتائج کی بنیادی وجہ لوگوں کا اپنی زندگی اور دوسروں کی زندگی کے درمیان موازنہ کرنے کی عادت یا جبلت ہے۔ میک نے مزید بتایا کہ فیس بک نے ہمارے دوسرے لوگوں کے متعلق حقیقی زندگی کے تصورات کو بالکل تباہ کر دیا ہے۔ فیس بک پر ہم ہر کسی سے اپنی زندگی اور طرز زندگی کا مقابلہ کرتے رہتے ہیں جو بے چینی کا سبب بنتا ہے۔ فیس بک پر لوگ اپنے بارے میں منفی چیزوں کے بجائے مثبت چیزیں پوسٹ کرتے ہیں۔ آج آپ کے دفتر میں باس نے آپ کو کس قدر جھاڑا، یہ چیز شاید آپ اپنے فیس بک پر شیئر نہ کریں۔ لیکن اسی دن آفس میں آپ نے کیا کھایا تھا، وہ شاید آپ شیئر کرنا نہ بھولیں۔ کسی کے گھر میں کس قدر ناچاکی چل رہی ہے، یہ بات بھی فیس بک پر نہیں آئے گی لیکن آئس کریم (چاہے وہ کسی اور نے کھلائی ہو) کھاتے ہوئے فوٹو اپ لوڈ کرنا لوگ نہیں بھولتے۔ اس سارے عمل کا نتیجہ یہ نکلتا ہے کہ دوسروں کے بارے میں ہمارا نظریہ حقیقت سے دور ہو جاتا ہے۔ اگر ہم ہمیشہ اچھی خبروں جو حقیقت کی ترجمانی نہیں کرتیں، کے جھرمٹ میں رہیں تو ہمیں اپنی زندگی کم اچھی لگنے لگتی ہے۔ مسٹر میک نے فیس بک کو خبروں کے ایک ایسے نان اسٹاپ ٹی وی چینل سے تشبیہ دی جو زندگی کی جھوٹی شکل پیش کرتا ہے۔

مسٹر میک کے مطابق انہیں امید ہے کہ اس تجربے کے نتائج سے فیس بک صارفین اس کے استعمال کے بارے میں ضرور غور کریں گے یا کم از کم وہ یہ ضرور یاد رکھیں گے کہ جو کچھ ان کی فیس بک نیوز فیڈ میں نظر آتا ہے وہ سب سچ یا حقیقت نہیں ہے۔

فیس بک پر کسی دوست کے متعلق ہمیں جو کچھ نظر آتا ہے وہ اس کی اصل زندگی میں ہونے والے واقعات کا دس فی صد ہوتا ہے۔ صرف اس دس فیصد کی بنیاد پر ہمیں اپنی زندگی کو نہیں پرکھنا چاہیے۔

نیا اینڈرائیڈ ایڈویئر، جو آپ کے فون کو روٹ کرنے کی کوشش کرتا ہے



انفارمیشن سکیوریٹی کمپنی لک آؤٹ نے ایک شاطر مال ویئر کے بارے میں انکشاف کیا ہے۔ یہ مال ویئر جسے شوانیٹ Shuanet کا نام دیا گیا ہے، دراصل ٹروجن کی ایک قسم ہے۔ لک آؤٹ کے مطابق انہوں نے اب تک اس مال ویئر کے 20 ہزار سے زیادہ نمونے تلاش کئے ہیں جو کینڈی کرش، فیس بک، گوگل ناؤ، ٹوئٹر، واٹس ایپ، ٹوئٹر اور اسنیپ چیٹ جیسی کثرت سے استعمال ہونے والی ایپلی کیشنز میں چھپے ہوئے تھے۔

شوانیٹ (Shuanet) صرف اشتہارات ہی نہیں دکھاتا، یہ ہر اس اینڈرائیڈ ڈیوائس کو روٹ کرنے کی کوشش کرتا ہے جس میں یہ انسٹال ہوجاتا ہے۔ کسی اینڈرائیڈ ڈیوائس کو روٹ کرنے کا مطلب ہوتا ہے کہ اس کا سکیوریٹی حصار توڑ کر سب سے طاقتور یوزر (جو روٹ یوزر کہلاتا ہے) کے حقوق حاصل کر لئے جائیں۔ روٹ کرنے کی وجہ سے یہ مال ویئر اس وقت بھی موبائل میں زندہ رہتا ہے جب صارفین اس سے بچنے کے لیے موبائل کو فیکٹری ری سیٹ کر دیتے ہیں۔

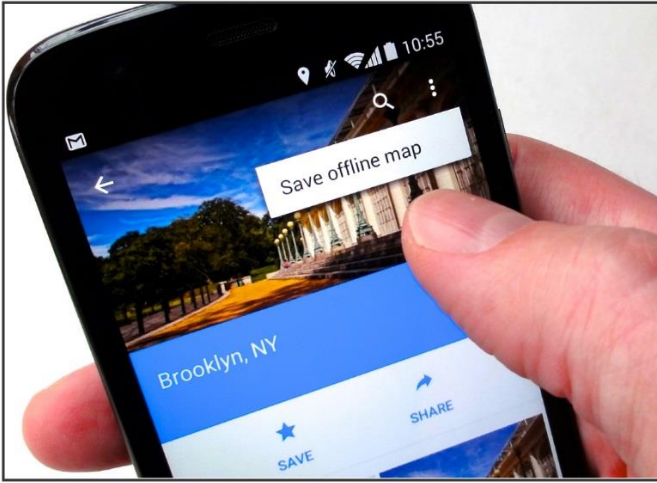
شوانیٹ کا سورس کوڈ دوسرے ایڈویئر ٹروجنز، جنہیں کیموگے (Kemoge) اور شیڈون (Shedun) کے نام سے شناخت کیا گیا ہے، جیسا ہی ہے۔ شوانیٹ کے بارے میں دلچسپ بات یہ ہے کہ دوسرے ٹروجن ہارسز کی طرح یہ متاثرہ ڈیوائس کو نئے وائرسوں سے بھر نہیں دیتا۔ کیونکہ اس کا بنیادی مقصد یہ نہیں کہ صارفین ڈیوائس استعمال ہی نہ کرسکیں۔ بلکہ یہ ٹروجن یا ایڈویئر چاہتا ہے کہ صارف اپنی ڈیوائس اور اس پر چلنے والی ایپلی کیشنز کو پہلے کی طرح استعمال کرتے رہیں تاکہ وہ انہیں اشتہار دکھا سکے۔

اس مال ویئر کے بنانے والے معروف ایپلی کیشن مثلاً فیس بک یا ٹوئٹر وغیرہ کی اے پی کے فائلوں کو گوگل پلے اسٹور سے ڈاؤن لوڈ کر کے ان میں مال ویئر پوشیدہ کر دیتے ہیں۔ پھر ان متاثرہ ایپلی کیشنز کو تھرڈ پارٹی ایپلی کیشن اسٹورز پر اپ لوڈ کر دیا جاتا ہے۔ جب کوئی صارف تھرڈ پارٹی ایپلی کیشن اسٹور سے ان متاثرہ ایپلی کیشنز کو ڈاؤن لوڈ کر کے استعمال کرتا ہے تو اسے بالکل محسوس نہیں ہوتا کہ یہ مال ویئر سے متاثرہ ہے۔ بظاہر یہ ایپلی کیشنز بالکل اصلی ایپلی کیشنز کی طرح کام کر رہی ہوتے ہیں جس سے صارف کو وائرس کا شبہ بھی نہیں ہوتا۔ تاہم یہ مال ویئر پاپ اپ کے ذریعے اشتہارات بھی دِکھانا شروع کر دیتا ہے اور صارف کو لگتا ہے کہ وہ ایپلی کیشنز ہی ان اشتہارات کی ذمے دار ہیں۔

بات اشتہارات دِکھانے تک رہتی تو یہ کسی حد تک قابل قبول تھی۔ لیکن شوانیٹ کا سب سے خطرناک پہلو ڈیوائس کو روٹ کرنے کی کوشش کرنا ہے۔ یہ انسٹال ہونے کے بعد ڈیوائس کو روٹ کرنے کے لئے کوئی خفیہ سسٹم یا اینڈرائیڈ سسٹم کی اچھوتی اور نئی قسم کی خرابی کا استعمال نہیں کرتا بلکہ یہ انہیں پرانی تکنیکس کا استعمال کرتا ہے جو لوگ اپنے اینڈرائیڈ فون یا ٹیبلٹ کو روٹ کرنے کے لئے استعمال کرتے ہیں۔ اگر شوانیٹ ڈیوائس کو روٹ کرنے میں کامیاب ہوجائے تو یہ متاثرہ ایپلی کیشن کو سسٹم پارٹیشن میں منتقل کر دیتی ہے۔ جس کا مطلب یہ ہے کہ اگر ڈیوائس کو Restore to Factory بھی کر دیا جائے تو بھی متاثرہ ایپلی کیشن ڈیوائس میں موجود رہتی ہے اور اسے ختم کرنے کے لئے کسی پروفیشنل کی مدد درکار ہوتی ہے۔

اس مال ویئر کی چالاکیاں خطرناک ضرور ہیں، لیکن اینڈرائیڈ صارفین کے لئے زیادہ پریشانی کی بات نہیں۔ اول تو بہت کم لوگ تھرڈ پارٹی ایپلی کیشن اسٹور سے ایپلی کیشنز ڈاؤن لوڈ کرتے ہیں، دوسرا یہ مال ویئر صرف انہیں ڈیوائسز کو متاثر کرتا ہے جو کہ اینڈرائیڈ کا پرانا ورژن مثلاً جیلی بین وغیرہ استعمال کر رہی ہیں۔ اس لئے اس مال ویئر سے پریشان ہونے کی قطعی ضرورت نہیں۔ البتہ انفارمیشن سکیوریٹی سے وابستہ افراد کے لئے یہ بات بہت پریشان کن ہے کہ مال ویئر اب ڈیوائسز کو روٹ کرنے کی کوشش بھی کرنے لگے ہیں۔ یہ عین ممکن ہے کہ مستقبل میں کوئی ایسا مال ویئر بھی آجائے تو اینڈرائیڈ کے نئے ورژن کو بھی روٹ کر سکتا ہو۔

اب گوگل میپس کو آف لائن رہتے ہوئے بھی استعمال کیا جاسکتا ہے



کسی انجان مقام پر پہنچنا ہو یا کسی جگہ کی تلاش ہو یا کسی مقام کا طائرانہ جائزہ لینا ہو، گوگل میپس ویب اور ایپلی کیشن دونوں صورتوں میں لاکھوں لوگوں کی پہلی ترجیح ہوتی ہے۔ لیکن صارفین نے ہمیشہ اس کی ایک خامی کا تذکرہ کیا ہے اور وہ خامی ہے اس کا بغیر انٹرنیٹ کے کام نہ کرنا۔ آخر کار گوگل نے گوگل میپس کے صارفین کی اس دیرینہ خواہش کو پورا کر ہی دیا۔ اب گوگل میپس کو آن لائن کے علاوہ آف لائن رہتے ہوئے بھی استعمال کیا جاسکتا ہے۔

گوگل میپس کی تازہ ترین اپ ڈیٹ کے مطابق صارفین اپنے قرب وجوار میں واقع مقامات کو بغیر انٹرنیٹ کے بھی تلاش کر کے وہاں تک جانے کا رستہ تلاش کر سکتے ہیں۔ گوگل نے گوگل میپس میں اس تبدیلی کا اعلان 6 ماہ پہلے آئی او 2015 کانفرنس کے موقع پر کیا تھا۔ گوگل کا کہنا ہے یہ فیچر ابھی صرف اینڈرائیڈ فونز میں متعارف کرایا گیا ہے۔ آئی او ایس کے لیے اسے جلد ہی جاری کر دیا جائے گا۔

گوگل کا کہنا ہے کہ وہ ترقی پذیر ممالک کے صارفین کے لیے زیادہ سے زیادہ سہولیات متعارف کرائے گا۔ آف لائن میپ کا فیچر بھی اسی ابھرتی ہوئی موبائل مارکیٹس کے لیے متعارف کرایا گیا ہے جہاں انٹرنیٹ بہت محدود اور کافی مہنگا ہے۔

ونڈوز فونز میں نقشوں کے لئے موجود ایپلی کیشن میں آف لائن میپس کا فیچر کافی پرانا تھا مگر ونڈوز فون کی مارکیٹ اینڈرائیڈ یا آئی فون کے مقابلے میں کافی چھوٹی ہے۔ آف لائن نقشوں کی سہولت تھرڈ پارٹی ایپلی کیشن کی مدد سے بھی استعمال کی جاسکتی ہے۔ ان میں نوکیا کی ہیر (Here) ایپلی کیشن کافی اہم ہے۔

گوگل میپ میں آف لائن میپ کے محدود فیچر متعارف کرائے گئے ہیں۔ اس میں چھوٹے اور مخصوص علاقے کے نقشے کو ہی آف لائن استعمال کے لیے محفوظ کیا جا سکتا ہے۔ کچھ اور محدود فیچرز کے باوجود آف لائن میپ کو بھی ایسے ہی استعمال کیا جاسکتا ہے جیسے آن لائن میپ کو۔

گوگل آف لائن میپس کو استعمال کرنے کے لیے کے آن لائن رہتے ہوئے گوگل میپس کا ڈیٹا بیس ڈاؤن لوڈ کرنا پڑتا ہے۔ ایسا کرنے کے لیے آپ اس مقام کا تعین کریں جہاں کا آف لائن ڈیٹا درکار ہو۔ زیادہ بڑے علاقے کو منتخب کرنے کی صورت میں ڈیٹا فائل کو فون میں زیادہ اسٹوریج درکار ہوگی۔ آپ جیسے ہی علاقے کا انتخاب کریں گے گوگل آپ کو بتائے کہ ڈیٹا فائل کا سائز کتنا ہے اور آپ کے موبائل میں کتنی جگہ بچی ہے۔ ایک بار ڈیٹا ڈاؤن لوڈ ہونے کے بعد گوگل وقتاً فوقتاً اس ڈیٹا بیس کو نئے کاروبار اور سڑکوں میں ہونے والی تبدیلیوں کے باعث اپ ڈیٹ کرتا رہے گا۔ بنیادی سیٹنگ کے مطابق گوگل صرف اس وقت ڈیٹا بیس کو اپ ڈیٹ کرے گا جب صارفین وائی فائی سے جڑے ہوں۔

آف لائن میپس میں ٹریفک کی معلومات دستیاب نہیں ہوتیں اور اس میں کاروبار کی تصاویر شامل ہوتی ہیں نہ کاروبار پر صارفین کے تبصرے۔ لیکن صارفین کاروبار کے رابطے کی معلومات، کاروباری اوقات اور صارفین کی طرف سے مجموعی ریٹنگ کی معلومات کے بارے میں جان سکتے ہیں۔

آف لائن میپس میں سمت بتانے کے فیچر ابتدائی طور پر ڈرائیونگ کے لیے ہیں۔ انہیں ابھی چہل قدمی، موٹر بائیک اور پبلک ٹرانسپورٹ کے لیے جاری نہیں کیا گیا۔ گوگل کا کہنا ہے کہ اس وقت دنیا کا 60 فیصد حصہ انٹرنیٹ کے بغیر ہے اور جہاں موجود ہے وہاں بھی اکثر جگہوں پر رفتار کے ساتھ کچھ اور مسائل کا شکار ہے۔ یعنی آبادی کی اکثریت کے لیے معلومات کی فوری رسائی ممکن نہیں۔ اسی وجہ سے لوگوں کو اپنے اردگرد کے علاقوں کو کھوجنے میں بھی مشکلات کا سامنا ہے۔ گوگل کا کہنا ہے کہ اب آپ دنیا کے کسی بھی مخصوص علاقے کو ڈاؤن لوڈ کر کے آف لائن استعمال کر سکتے ہیں۔ چاہے یہ علاقہ کوئی سڑک ہو یا پھر انڈر گراؤنڈ پارکنگ گیراج۔ گوگل کا کہنا ہے کہ آن لائن میپ بھی اسی طرح کام کرتا رہے گا۔

فضائی آلودگی کے مضر اثرات سے بچاؤ کے لئے سینسر تیار، اسمارٹ فون میں بھی نصب کیا جاسکتا ہے



فضائی آلودگی ایک عالمی مسئلہ ہے جس نے عالمی طاقتوں کے ناک میں دم کررکھا ہے۔ ورلڈ ہیلتھ آرگنائزیشن کے مطابق زہریلی فضائی آلودگی کی وجہ سے ہر سال ستر لاکھ سے بھی زیادہ افراد، جن میں بڑی تعداد بچوں کی ہوتی ہے، موت کے منہ میں چلتے جاتے ہیں۔ زہریلی گیسیں بچوں اور بوڑھوں میں نظام تنفس کی مہلک بیماریوں کے خطرات بھی بڑھادیتی ہیں۔

فضائی آلودگی پر قابو پانے کے لئے دنیا بھر کی حکومتیں کوشش کررہی ہیں اور یہ کوششیں کافی حدتک سودمند بھی ثابت ہورہی ہیں۔ لیکن عوام کے لئے یہ جاننے کا کوئی طریقہ نہیں کہ جس علاقے میں وہ رہ رہے ہیں، وہ کس قدر آلودہ ہے۔ بیشتر زہریلی گیسیں (مثلاً کاربن مونو آکسائیڈ) بے بو اور بے ذائقہ ہوتی ہیں جس کی وجہ سے انسانی ناک اُن کا پتا نہیں چلاپاتی۔ جس کی وجہ سے انسان زہریلی گیسوں میں ایک لمبے عرصے تک گھرا رہتا ہے جو صحت پر گہرا اثر ڈالتی ہیں۔

اب اس ضمن میں ایک اہم کامیابی آسٹریلیا کی آر ایم آئی ٹی یونیورسٹی کے محققین کو حاصل ہوئی ہے۔ اس یونی ورسٹی کے سینٹر فار ایڈوانسڈ الیکٹرونکس اینڈ سینسرز کے ماہرین نے ایک سستا اور حساس سینسر تیار کرنے میں کامیاب ہوگئے ہیں جو فضا میں موجود زہریلی نائٹروجن ڈائی آکسائیڈ گیس کی مقدار بتا سکتا ہے۔ دلچسپ بات یہ ہے کہ اس سینسر کو اسمارٹ فون میں بھی نصب کیا جاسکتا ہے۔ یعنی جلد ہی ماحولیات کے حوالے 100 فیصد درست ڈیٹا جمع کرنا آسان ہوجائے گا۔

اس سینسر کے کام کرنے کا طریقہ کچھ یوں ہے کہ یہ فضا میں نائٹروجن ڈائی آکسائیڈ گیس کے مالیکیول کو ٹن ڈائی سلفائیڈ کے انتہائی چھوٹے ٹکڑوں یا نقطوں پر جذب کرتا ہے۔ ٹن ڈائی سلفائیڈ کا رنگ قدرتی طور پر پیلا بھورا ہوتا ہے اور اسے سجاوٹ اور تزین و آرائش کے لئے بطور رنگ استعمال کیا جاتا ہے۔ سینسر بنانے کے لیے محققین نے ٹن ڈائی آکسائیڈ کو نقطے یا دھبے جیسی شکل میں ڈھالا۔ ان نقطوں کی موٹائی چند ایٹموں سے زیادہ نہیں تھی۔ ان نقطوں کی سطح نائٹروجن ڈائی آکسائیڈ کے مالیکیول جذب کرکے درست ڈیٹا فراہم کرنے کے لئے بہترین ہے۔ اس سینسر کے بارے میں اسے بنانے والی ٹیم کا دعویٰ ہے کہ یہ نائٹروجن ڈائی آکسائیڈ کی موجودگی کی خبر دینے والے کسی بھی دوسرے سینسر کے مقابلے میں زیادہ حساس اور درست ہے۔

پروفیسر کوروش کالانٹر زادہ (Kourosh Kalantar-Zadeh)، جو اس پراجیکٹ کے سربراہ ہیں، نے کہا کہ ہم ذاتی، حساس اور قابل اعتماد ڈیٹا تک رسائی حاصل کرکے نائٹروجن ڈائی آکسائیڈ گیس کے نقصان دہ اثرات سے بچ سکتے ہیں۔ انہوں نے مزید بتایا کہ اس انقلابی طریقے سے ہم نے ایسے سستے اور چھوٹے سینسر بنالئے ہیں جنہیں اسمارٹ فون میں بھی نصب کیا جاسکتا ہے۔ اسمارٹ فون میں تنصیب سے اس سینسر کے ذریعے لاکھوں لوگوں کے اردگرد موجود نائٹروجن ڈائی آکسائیڈ کی مقدار کا ڈیٹا جمع کیا جاسکے گا۔ اس سے نہ صرف لاکھوں افراد کا معیار زندگی بہتر ہوگا بلکہ لوگ نائٹروجن ڈائی آکسائیڈ کے زہریلے اثرات سے بھی محفوظ رہ سکیں گے۔ پروفیسر کالانٹر نے اس سینسر کو اپنے ساتھیوں اور چینی اکیڈمی آف سائنس کے رفقاء کے ساتھ مل کر بنایا ہے۔ اس منصوبے کا مرکزی خیال یہ تھا کہ کسی طرح فضائی آلودگی کے ڈیٹا کو عام عوام کی پہنچ میں لایا جائے تاکہ اسے فضائی آلودگی سے بچنے کے لیے استعمال کیا جاسکے۔ کالانٹر کے مطابق اس وقت نائٹروجن ڈائی آکسائیڈ کی موجودگی کی خبر دینے والے جو سینسر موجود ہیں وہ یا تو بہت مہنگے ہیں یا پھر وہ نائٹروجن ڈائی آکسائیڈ کو فضاء میں موجود دوسری گیسوں سے الگ پہچاننے میں ناکام رہتے ہیں۔

فضاء میں نائٹروجن ڈائی آکسائیڈ کی بڑی وجہ کوئلے سے چلنے والے بجلی گھر اور آلات، حیاتیاتی ایندھن کا جلنا اور ڈیزل انجن ہیں۔ حال ہی میں معروف گاڑی ساز کمپنی واکس ویگن کو دنیا بھر میں شرمندگی کا سامنا کرنا پڑا جب ان کی گاڑیوں سے خارج ہونے والی آلودگی کے بارے میں بتایا گیا جھوٹ دنیا کے سامنے آگیا۔

انڈونیشیاء میں بھی گوگل کے پروجیکٹ لون کا آغاز



گوگل انڈونیشیاء کے شہریوں تک تیز رفتار انٹرنیٹ پہنچانے کے لیے پراجیکٹ لون کے تحت انڈونیشیاء میں ہزاروں ہوائی غبارے فضاؤں میں بلند کرے گا۔ گوگل انڈونیشیاء کے ٹیلی کام آپریٹرز کے ساتھ مل کر خطے کے دس کروڑ سے زائد لوگوں کو تیز ترین LTE کنکشن مہیا کرنا چاہتا ہے۔ اس مقصد کے لیے گوگل نے انڈونیشیاء کے ٹیلی کام آپریٹر Indosat، Telkomsel اور XL Axiata کے ساتھ ایک یادداشت پر دستخط کیے ہیں۔ انڈونیشیاء میں گوگل کے پراجیکٹ لون کے تحت انٹرنیٹ کی فراہمی کے تجربات اگلے سال شروع ہونگے۔

افریقا کے بہت سے ممالک اور ایشیاء کے دیگر علاقوں کے مقابلے میں انڈونیشیاء میں انٹرنیٹ تک رسائی رکھنے والوں کی تعداد زیادہ ہے۔ لیکن جنوب مشرقی ایشیائی ممالک میں لوگ ابھی بھی انٹرنیٹ سے محروم ہیں۔ ایک اندازے کے مطابق جنوب مشرقی ایشیائی اقوام کی مجموعی آبادی 25 کروڑ 60 لاکھ ہے جو سترہ ہزار جزیروں پر رہتی ہے۔ مقامی اعداد و شمار کے مطابق ان میں سے ایک تہائی افراد کی انٹرنیٹ تک رسائی ہے لیکن انٹرنیٹ سوسائٹی ڈاٹ آرگ کے اندازوں کے مطابق انڈونیشیاء کا انٹرنیٹ 15.8 فیصد صارفین کے ساتھ دنیا میں صارفین کے لیے 135 واں نمبر ہے۔

گوگل نے دو سال پہلے پراجیکٹ لون کا آغاز کیا تھا۔ اس پراجیکٹ کے تحت گوگل فضا میں ہزاروں غباروں کی مدد سے ایسے علاقوں میں تیز رفتار انٹرنیٹ پہنچائے گا جہاں تک روایتی طریقوں سے انٹرنیٹ کی فراہمی ممکن نہیں۔ گوگل کے غبارے سطح زمین سے 18 ہزار میٹر بلندی پر رہ کر زمین پر انٹرنیٹ سروسز مہیا کریں گے اور ہر غبارہ سورج کی روشنی سے اپنی توانائی کی ضروریات پوری کرے گا۔ ایک مقام سے دوسرے مقام تک پہنچنے کے لئے یہ غبارے ہوا کا سہارا لیتے ہیں۔ انڈونیشیاء وہ چوتھا ملک ہوگا جہاں پراجیکٹ لون کو عملی شکل دی جائے گی۔ اس سے پہلے گوگل برازیل، آسٹریلیا اور نیوزی لینڈ میں پراجیکٹ لون کی آزمائش کر چکا ہے۔ 18 ہزار میٹر کی بلندی پر رہنے کی وجہ سے ان غباروں کے سگنلز کی رسائی ایک بڑے علاقے تک ہوتی ہے۔ ان میں وہ علاقے مثلاً جنگل، صحرا، پہاڑ یا سمندر بھی شامل ہیں جہاں انٹرنیٹ سرے سے دستیاب ہی نہیں یا بہت مشکل سے ہی دستیاب ہوسکتا ہے۔

پروجیکٹ لون کے لئے گوگل نے ہر ملک میں اپنا ذاتی فریکوئنسی اسپیکٹرم حاصل نہیں کیا۔ یہ بہت لمبا اور مہنگا کام ہے۔ اس کے بجائے گوگل مقامی ٹیلی کام آپریٹرز کی خدمات حاصل کرتا ہے اور ان کی سروسز استعمال کرتا ہے۔ زمین پر موجود انٹرنیٹ صارفین ایک خاص انٹینا کے ذریعے غبارے سے جڑے ہوتے ہیں جبکہ غبارہ ٹیلی کام آپریٹر کے زمین پر بیس اسٹیشن سے جڑا ہوتا ہے۔ یوں صارفین غبارے کے ذریعے مقامی ٹیلی کام آپریٹر کا انٹرنیٹ استعمال کرتے ہیں۔

ماہرین کا کہنا ہے کہ جغرافیائی اعتبار سے انڈونیشیاء میں انٹرنیٹ کی فراہمی ایک مشکل امر ہے۔ یہ خطہ ہزاروں جزیروں پر محیط ہے اور ہر جزیرے تک عام دستیاب ٹیکنالوجی کے ذریعے انٹرنیٹ فراہم کرنا بہت جان جوکھوں کا کام ثابت ہوتا ہے۔ اسی چیز کو مدنظر رکھتے ہوئے گوگل کا کہنا ہے کہ پروجیکٹ لُون انڈونیشیاء کی اس مشکل کو آسان بنائے گا۔ پروجیکٹ لون کے نائب صدر مائک کسیڈی کا کہنا ہے کہ لُون کے ذریعے ٹیلی کمیونی کیشن کمپنیاں اپنے نیٹ ورک کو مزید پھیلا سکیں گی۔

گوگل کا مشن ہے کہ وہ اگلے پانچ سالوں میں کم از کم دس کروڑ ایسے لوگوں تک انٹرنیٹ پہنچائے گا جنہیں انٹرنیٹ دستیاب نہیں۔ اسی کوشش میں گوگل پروجیکٹ لون کو نیومیکسیکو، چلی اور سری لنکا میں بھی ٹیسٹ کر چکا ہے۔ ایک الگ پروجیکٹ کے تحت گوگل نے حال ہی میں اعلان کیا تھا کہ وہ بھارت کے 400 سے زائد ریلوے اسٹیشنوں پر تیز رفتار اور مفت وائی فائی کی سروس فراہم کرے گا۔

گوگل کے پروجیکٹ لون جیسا ہی ایک پروجیکٹ فیس بک نے بھی شروع کر رکھا ہے۔ لیکن اس میں غباروں کے بجائے ڈرونز کا استعمال کیا جاتا ہے۔ ان دونوں کمپنیوں کا کاروبار انٹرنیٹ صارفین کے دم سے ہی ہے۔ اس لئے یہ دونوں انٹرنیٹ صارفین کی تعداد میں اضافہ کرنے کے لئے کوشاں ہیں۔

گوگل نے اپنا مصنوعی ذہانت کا پروجیکٹ اوپن سورس کردیا



ہمارے اسمارٹ فونز اور کمپیوٹر بے شک ذہین ہو گئے ہیں تاہم ان میں انسانی دماغ جتنی طاقت، کارکردگی اور ذہانت ابھی نہیں ہے۔اسی مسئلے کو حل کرنے کے لیے گوگل سمیت درجنوں بڑی کمپنیاں اور جامعات کے تحقیقی مراکز سر توڑ کوشش کر رہے ہیں۔ایک ایسا کمپیوٹر جو انسانی دماغ جتنا ذہین ہو،ایک خواب کی مانند ہے جو اگر حقیقت کا روپ دھار لیتا ہے تو یہ انسانی کی اب تک کی سب سے بڑی کامیابی گردانا جائے گا۔ایسے ذہین کمپیوٹر عملی طور پر انسانوں کے رہنے سہنے کے طور طریقوں کو بدل کر رکھ دیں گے۔

کئی سالوں سے انجینئر انسانی دماغ کی نقل کرنے کے لیے ڈیپ نیورل نیٹ ورکس ڈیزائن کرنے میں لگے ہوئے ہیں۔گوگل کی تحقیق اس حوالے سے خاصی نمایاں ہے۔گوگل نے سال 2011ء میں گوگل برین نامی پروجیکٹ کا آغاز کیا تھا۔اس پروجیکٹ کے تحت مشین لرننگ نظام DisBelief تیار کیا گیا۔اس ذہین نظام کو گوگل نے اپنے تمام اہم مصنوعات جن میں گوگل سرچ، گوگل وائس سرچ، گوگل فوٹوز، گوگل میپس، گوگل ٹرانسلیٹر اور یوٹیوب بھی شامل ہیں، میں استعمال کیا گیا۔ڈاکٹر جیف ڈین جیسے نامی گرامی کمپیوٹر سائنس دانوں اس پروجیکٹ کا حصہ تھے جنھیں ڈِس بلیف کو تیز رفتار اور اعلیٰ قسم کی لائبریری کی شکل میں ڈھالنے کا کام سونپا گیا تھا۔ڈِس بلیف ہی بہتری کے بعد ٹینسر فلو(TensorFlow) بنا جو گوگل برین کے مشین لرننگ سسٹم کی دوسری نسل ہے۔یہ مشین لرننگ سسٹم ڈیپ لرننگ تکنیک استعمال کرتے ہیں۔مثلاً اس نظام کو سینکڑوں یا ہزاروں بلیوں یا کتوں کے فوٹو فراہم کئے جائیں تو یہ ان تصاویر کی مدد سے بلی یا کتے کو پہچاننا سیکھ جاتا ہے۔پھر اسے اگر کوئی ایسی تصویر دی جائے جو پہلے اسے فراہم نہیں کی گئی تھی، تو یہ اس میں سے بھی کتے یا بلی کو شناخت کرسکتا ہے۔

اب گوگل نے ایک بڑا اور حیران کن قدم اٹھاتے ہوئے، ٹینسر فلو(TensorFlow) کو ہر خاص و عام کے لئے دستیاب کر دیا ہے۔اسے آپاچی 2.0 اوپن سورس لائسنس کے تحت جاری کیا گیا ہے۔دنیا بھر میں مصنوعی ذہانت پر تحقیق کرنے والے سائنس دانوں نے گوگل کے اس اقدام کی زبردست پذیرائی کی ہے اور اسے مصنوعی ذہانت میں ترقی کی رفتار بڑھانے کا سبب قرار دیا ہے۔جبکہ گوگل کا کہنا ہے کہ ٹینسر فلو کو اوپن سورس کرنے سے نئے سافٹ ویئر زیادہ ذہین اور بہتر ہو جائیں گے۔

گوگل کے سی ای او سندر پچائی کا کہنا ہے کہ کچھ سالوں پہلے تک گوگل ایپلی کیشن سے بات نہیں کی جاسکتی ہے۔گوگل مترجم روسی زبان کے سائن بورڈ نہیں پڑھ سکتا تھا نہ ہی ہماری ایپلی کیشن اتنی زیادہ ذہین تھیں۔لیکن قلیل وقت میں ہم نے کافی کچھ حاصل کرلیا اور ہماری ایپلی کیشنز اب زیادہ ذہین ہوگئیں ہیں۔مشین لرنگ کا شکریہ جس کی مدد سے پہلے ناممکن سمجھے جانے والے کام آسانی سے سرانجام دیئے جاسکتے ہیں اور یہ اور بھی بہتر انداز سے کام کرسکتا ہے۔

گوگل اس وقت ٹینسر فلو کو اپنی ایپلی کیشنز میں آواز کی شناخت کے لیے استعمال کر رہا ہے۔ان بکس ایپلی کیشن میں اسمارٹ ریپلائی اور گوگل فوٹوز میں سرچ کے فیچرز بھی ٹینسر فلو کی ہی مرہون منت ہیں۔سندر پچائی کا کہنا ہے کہ ہم نے دیکھ لیا ہے کہ ٹینسر فلو کیا کرسکتا ہے لیکن ہمیں یقین ہے کہ یہ گوگل سے باہر بھی بڑے اہم کام کرے گا۔اس کا کہنا تھا کہ یہ سسٹم مشین لرنگ کو طالب علموں سے لیکر انجینئروں اور مشین لرنگ کا شوق رکھنے والوں، سب کے لیے آسان بنا دے گا۔مشین لرنگ اور ڈیپ نیورل نیٹ ورکس کی تازہ ترین مثال گوگل کی طرف سے بنایا گیا conversation ماڈل اور ڈیپ ڈریم پروگرام ہے۔

حالیہ سالوں میں گوگل کے علاوہ دوسری کمپنیوں مثلاً فیس بک، مائیکروسافٹ اور ٹوئٹر نے بھی مصنوعی ذہانت کے میدان میں بڑی کامیابیاں حاصل کی ہیں۔کچھ نے تو اپنے مصنوعی ذہانت کے نظام اوپن سورس بھی کر رکھے ہیں۔اس کی ایک مثال Torch ہے جسے سوئزرلینڈ کے محققین نے تیار کیا ہے۔لیکن گوگل کا ٹینسر فلو ان سب سے زیادہ جدید اور ذہین ہے۔

فیس بک اب دے گا آپ کو ریاستی سرپرستی میں ہونے والے حملہ کی اطلاع

فیس بک کے کھاتے ہیکروں کے پسندیدہ شکار ہیں۔ فیس بک پر فعال کسی شخص کا فیس بک اکاؤنٹ اس شخص کے حوالے سے خزانے جتنی معلومات رکھتا ہے۔ اس لئے دنیا کے طاقتور ممالک اور فیس بک کے درمیان رسہ کشی جاری رہتی ہے کیونکہ ان ممالک کے لئے کسی شخص کی نجی معلومات تک رسائی کے لئے فیس بک سب سے آسان طریقہ ہے۔

اب فیس بک نے اپنے صارفین کے کھاتوں کو مزید محفوظ بنانے کے لئے اعلان کیا ہے کہ وہ ان تمام صارفین کو ایک نوٹیفکیشن کے ذریعے مطلع کرے گا جن کے کھاتوں کو کسی ریاستی سرپرستی کے تحت ہیک کرنے کی کوشش کی جارہی ہو۔ اس حوالے سے اپنی بلاگ پوسٹ میں فیس بک نے کہا کہ اگرچہ ہم ایسے تمام اکاؤنٹس کے حفاظت کے لئے مناسب اقدامات کرتے ہیں جن کے بارے میں ہمیں یقین ہو کہ وہ ہیک کر لئے گئے ہیں۔ تاہم اب ہم نے فیصلہ کیا کہ ایسے تمام صارفین کو ایک اضافی انتباہی نوٹی فکیشن دیا جائے جن کے اکاؤنٹس کے بارے میں ہمیں شبہ ہو کہ ان پر کسی ریاست کی سرپرستی میں حملہ کیا جارہا ہے۔ ہم ایسا اس لئے کر رہے ہیں کیونکہ اس نوعیت کے حملے زیادہ جدید اور خطرناک ہوتے ہیں۔ فیس بک نے اپنی بلاگ پوسٹ میں یہ بھی کہا ہے کہ اس نوٹیفکیشن کا مطلب ہرگز یہ نہیں کہ پورا فیس بک ہی کسی ریاستی سرپرستی میں کام کرنے والے ہیکروں نے ہیک کرلیا ہے۔ اگرچہ اس قسم کا نوٹی فکیشن ہم میں سے بیشتر لوگ کبھی نہ دیکھیں۔ لیکن اگر آپ کو ایسا کوئی نوٹی فکیشن نظر آتا ہے تو فی الفور اپنے فیس بک اور دیگر آن لائن کھاتوں کے پاس ورڈ تبدیل کر کے زیادہ مشکل پاس ورڈ استعمال کریں۔



Please Secure Your Accounts Now

Jay, we believe your Facebook account and your other online accounts may be the target of attacks from state-sponsored actors. Turning on Login Approvals will help keep others from logging into your Facebook account. Whenever your account is accessed from a new device or browser, we'll send a security code to your phone so that only you can log in. We recommend you also take steps to secure the accounts you use on other services. Learn more.

Turn on Login Approvals

گوگل اپنا اسمارٹ فون بنا سکتا ہے



گوگل کے بارے میں دی انفارمیشن نامی ویب سائٹ نے خبر دی ہے کہ کمپنی کے اندر اپنا اسمارٹ فون تیار کرنے کے منصوبے پر بحث جاری ہے۔ اگر ایسا ہوا تو یہ کوئی انہونی بات نہیں ہوگی کیونکہ گوگل پہلے ہی کروم بک پکسل اور پکسل سی ٹیبلٹ کے لئے ہارڈ ویئر تیار کر رہا ہے۔ تاہم گوگل اسمارٹ فون نہیں بناتا اور اس کے نیکسس سیریز کے فون اور ٹیبلٹ دوسرے اسمارٹ فون بنانے والی کمپنیاں تیار کرتی ہیں۔ یہ خبر اس لئے بھی اہمیت رکھتی ہے کیونکہ حال ہی میں ایک خبر یہ بھی آئی تھی کہ گوگل اپنا مائیکرو پروسیسر ڈیزائن کرنے کے لئے بات چیت کر رہا ہے۔

دی انفارمیشن نے اس بات پر زور دیا ہے کہ گوگل نے اس حوالے سے ابھی تک حتمی طور پر فیصلہ نہیں کیا۔ کیونکہ ایسا کرنے کے نتائج بہت خراب بھی ہو سکتے ہیں۔ سب سے بڑا خطرہ یہ ہے کہ گوگل کے لئے اسمارٹ فون بنانے والی کمپنیوں اور گوگل کے تعلقات خراب ہو سکتے ہیں۔ گوگل اگر اپنا اسمارٹ فون تیار کرنے کا فیصلہ کرتا ہے تو یہ سام سنگ جیسی کمپنیوں کے ساتھ براہ راست ٹکراؤ ہوگا۔

اگلے ایک ارب اسمارٹ فونز کے لئے ARM کی نئی 64 بٹ چپ

Cortex-A17 Cortex-A15	Cortex-A72 Cortex-A57	High Performance
Cortex-A9	Cortex-A53	High Efficiency
Cortex-A7 Cortex-A5	Cortex-A35	Ultra High Efficiency
ARMv7-A	ARMv8-A	

ARM نے ایک نئے ڈیزائن کا اجراء کیا ہے جس کے بارے میں کمپنی کا دعویٰ ہے کہ وہ بھارت، چین اور برازیل جیسے ممالک جہاں اسمارٹ فونز کی زبردست مانگ ہے، میں سستے لیکن اعلیٰ کارکردگی کے حامل اسمارٹ فونز کی وجہ بنے گا۔

ترقی یافتہ اور امیر ممالک میں اسمارٹ فون خریدنے کے خواہش مند لوگوں کے پاس پہلے ہی اسمارٹ فون موجود ہوتا ہے۔ اس لئے مہنگے، زبردست ہارڈویئر اور سافٹ ویئر رکھنے والے اسمارٹ فونز کی مانگ میں کمی واقع ہورہی ہے۔ لیکن ترقی پذیر ممالک میں اس کے برعکس اسمارٹ فونز کی مانگ میں زبردست اضافہ دیکھنے میں آیا ہے اور ARM کی نئی چپ بھی اسی مارکیٹ کو مدنظر رکھتے ہوئے تیار کی گئی ہے۔

اس نئی چپ جسے Cortex-A35 کا نام دیا گیا ہے، کمپنی کی پہلی چپ ہے جو ARMv8 آرکیٹیکچر پر مبنی ہے اور اسے کم قیمت اسمارٹ فونز کے لئے تیار کیا گیا ہے۔ ARMv8 پہلے ہی مہنگے اور طاقتور اسمارٹ فونز جیسے آئی فون 6S میں استعمال کیا جارہا ہے اور یہ 64 بٹ پروسیسر ہے۔

اگرچہ اس حوالے سے لمبے بحث ومباحثے چل رہے ہیں کہ آیا اسمارٹ فونز میں 64 بٹ پروسیسرز کا کوئی فائدہ ہے بھی کہ نہیں۔ لیکن ARM کا دعویٰ ہے کہ نئی چپ کی وجہ سے مختلف ایپلی کیشنز کی کارکردگی میں قابل ذکر حد تک اضافہ دیکھا گیا ہے۔ Cortext A7 کے مقابلے میں اس نئی چپ کی کارکردگی 20 فی صد تک بہتر ہے۔ تاہم اس کا بڑا انحصار ایپلی کیشن پر بھی ہے۔

کم توانائی خرچ کرنا اے آر ایم چپس کا ہمیشہ سے خاصا رہا ہے اور اسی وجہ سے یہ چپ اسمارٹ فونز میں اس قدر کامیاب ثابت ہوئی ہے۔ کورٹیکس اے 35 بھی اس معاملے میں آگے ہیں۔ تفصیلات کے مطابق ایک گیگا ہرٹز کی کلاک اسپیڈ پر کام کرتے ہوئے اے 35 جسے 28 نینومیٹر پروسس پر تیار کیا گیا ہو، صرف 90 ملی واٹ فی کور بجلی خرچ کرتی ہے۔ یعنی اس چپ پر مبنی اسمارٹ فونز کی بیٹری زیادہ وقت تک چلتی رہے گی۔ یاد رہے کہ آج کل کے اسمارٹ فونز میں استعمال ہونے والی چپس 28 نینومیٹر پروسس پر ہی تیار کی جاتی ہیں۔

کورٹیکس اے 35 صرف سستے اور کم طاقتور اسمارٹ فونز کے لئے نہیں ہے بلکہ ARM اسے big.Little کنفگریشن کی صورت میں بھی استعمال کرنا چاہتا ہے۔ big.Little دراصل طاقتور اسمارٹ فونز کے لئے تیار کی گئی چپس میں استعمال ہونے والی ایک تکنیک ہے۔ اس میں ایک طاقتور پروسیسر کے ساتھ ایک کم طاقتور پروسیسر بھی لگایا جاتا ہے۔ ویڈیو چلانے یا ایسے کاموں جن میں زیادہ کمپیوٹنگ پاور درکار ہوتی ہے، پروسیسر کی طاقتور core استعمال کی جاتی ہے لیکن ای میل چیک کرنے جیسے معمولی کاموں کے لئے کم طاقتور پروسیسر استعمال کیا جاتا ہے جس سے بیٹری کی بڑی بچت ہوتی ہے۔

ARM بذات خود مائیکرو پروسیسر یا سسٹم آن چپ نہیں بناتی۔ بلکہ یہ کمپنی صرف پروسیسر یا چپ کا ڈیزائن تیار کرتی ہے اور مائیکرو چپس بنانے والی کمپنیاں ان سے لائسنس فیس کے عوض ڈیزائن خریدتی ہیں۔ کمپنی بنیادی طور پر دو طرح کے لائسنس فروخت کرتی ہے۔ architectural اور پروسیسر۔ ایپل اور سام سنگ جیسی کمپنیاں ان سے architectural لائسنس خریدتی ہیں اور ARM کے آرکیٹیکچر کی بنیاد پر اپنا پروسیسر خود تیار کرتی ہیں۔ ARM کمپنی مکمل پروسیسر بھی ڈیزائن کرتی ہے۔ یہی پروسیسر کورٹیکس سیریز کے پروسیسر ہوتے ہیں۔ مکمل ڈیزائن کا لائسنس خریدنے والی کمپنیاں پروسیسر کے ڈیزائن میں تبدیلیاں کرنے کی مجاز نہیں ہوتیں۔ لیکن اس قسم کے لائسنس کا فائدہ یہ ہے کہ ہارڈویئر بنانے والی کمپنیاں انتہائی تیزی سے نئی چپ مارکیٹ میں لاسکتی ہیں کیونکہ انہیں چپ ڈیزائن کرنے کی محنت نہیں کرنی پڑتی۔

ARM کا کہنا ہے کہ اب تک اس کے اینٹری لیول کورٹیکس A5 اور A7 چپس پر مبنی 2 ارب سے زائد اسمارٹ فونز تیار کئے جاچکے ہیں۔

مائیکروسافٹ کا لینکس کے لئے پیار یا کاروباری چال؟

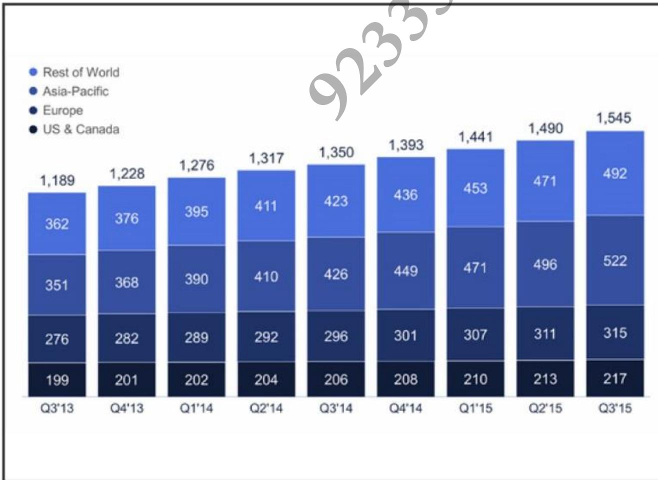


اے یور (Auzre) مائیکروسافٹ کی معروف کلاؤڈ سروس ہے جہاں ورچوئل مشینوں کے علاوہ ایس کیو ایل سرور ڈیٹا بیس بھی بنائے جاسکتے ہیں۔ مائیکروسافٹ اے یور پر دستیاب سہولیات میں دن بدن اضافہ کرنے کے لئے کوشاں ہے اور اس کے لئے مختلف کمپنیوں کے ساتھ اشتراک کرتا رہتا ہے۔ اب تازہ اطلاع کے مطابق مائیکروسافٹ اور لینکس آپریٹنگ سسٹم کے لئے معروف کمپنی ریڈ ہیٹ نے ایک معاہدہ کیا ہے جس کے تحت مائیکروسافٹ اے یور پر ریٹ ہیٹ انٹرپرائز لینکس بھی استعمال کرنے کے لئے دستیاب ہوگی۔ یوں مائیکروسافٹ اے یور کے صارفین ایک دیرینہ خواہش بھی پوری ہوگئی۔

مائیکروسافٹ اے یور پر لینکس کی مختلف ڈسٹری بیوشنز پہلے ہی دستیاب ہیں۔لیکن ریڈ ہیٹ دستیاب نہ تھی۔ ریڈ ہیٹ لینکس کی معروف ترین ڈسٹری بیوشنز میں سے ایک ہے اور کارپوریٹ سطح پر ریڈ ہیٹ صارفین کی پہلی ترجیح ہوتی ہے۔ دیگر لینکس ڈسٹری بیوشنز کے برعکس ریڈ ہیٹ کی سپورٹ حاصل کرنا آسان ہے تاہم یہ مفت نہیں ہے۔

ماہرین کا خیال ہے کہ مائیکروسافٹ کو ریڈ ہیٹ کے ساتھ یہ معاہدہ بہت پہلے کرلینا چاہئے تھا۔ معروف ریسرچ کمپنی گارٹنر کے ریسرچ ڈائریکٹر Elias Khnaser کے مطابق یہ معاہدہ آج نہیں بلکہ 18 ماہ پہلے ہوجانا چاہئے تھا۔ ان کا مزید کہنا تھا کہ یہ خبر مائیکروسافٹ کی حریف مصنوعات سے بالاتر ہوکر سوچنے کی صلاحیت کی عکاس ہے۔ اس نئے معاہدے سے کسی بہت بڑی تبدیلی کی توقع نہیں۔ کیونکہ مائیکروسافٹ اے یور کی حریف سروس ایمزون ویب سروسز اس میدان میں مائیکروسافٹ سے بہت پہلے سے موجود ہے اور اس نے اپنے قدم مضبوطی سے جما رکھے ہیں۔

فیس بک نے ایک اور سنگ میل عبور کرلیا



فیس بک نے ستمبر 2012ء میں ایک اہم سنگ میل عبور کیا تھا۔ یہ سنگ میل فیس بک کے فعال ماہانہ صارفین کی تعداد ایک ارب تک پہنچنا تھا۔ اب تقریباً تین سال بعد فیس بک نے ایک اور سنگ میل عبور کرلیا ہے۔ فیس بک کے جاری بیان کے مطابق فیس بک کی تاریخ میں پہلی بار ماہانہ فعال صارفین کی تعداد ایک ارب پچاس کروڑ کے ہندسے کو پہنچ چکی ہے۔ اس سے پہلے پچاس کروڑ صارفین سے ایک ارب صارفین کا ہدف فیس بک نے صرف دو سال میں حاصل کرلیا تھا۔ موازنے کے لئے ہم بتاتے چلیں کہ ٹوئٹر کے ماہانہ فعال صارفین کی تعداد 32 کروڑ ہے۔

فیس بک اس سنگ میل کے بارے میں تیسری سہ ماہی کے مالیاتی نتائج کے اجراء کے موقع پر بتایا۔ مالیاتی نتائج کے مطابق فیس بک نے ایک بار پھر متوقع منافع سے زیادہ منافع کمایا۔ تیسری سہ ماہی کے دوران فیس بک نے ساڑھے چار ارب ڈالر کمائے جو گزشتہ سال کے مقابلے میں 41 فی صد زیادہ ہیں۔ خالص منافع گیارہ فیصد اضافے کے ساتھ 896 ملین ڈالر رہا۔

اینڈ رویئڈ کی سکیوریٹی خامیوں کی بڑی وجہ اسمارٹ فون بنانے والے ادارے ہیں



گوگل اینڈ رویئڈ مفت دستیاب ہے اور اسے کوئی بھی اپنی مرضی سے تبدیل کر کے استعمال کر سکتا ہے۔ نیز اس کے لئے کوئی لائسنس فیس بھی نہیں دینی پڑتی۔ یہ اس کی کامیابی کی ایک بڑی وجہ ہے۔ لیکن اس کی یہی خوبی اس کی ایک بڑی خرابی بھی ہے۔ اسمارٹ فون اور ٹیبلٹ بنانے والی کمپنیاں اینڈ رویئڈ آپریٹنگ سسٹم کو من و عن استعمال نہیں کرتیں بلکہ اس میں اکثر تبدیلیاں کر کے اسے اپنی مرضی کے مطابق ڈھالتی ہیں۔ ان تبدیلیوں کی وجہ سے اینڈ رویئڈ آپریٹنگ سسٹم کی سکیوریٹی پر گہرا اثر پڑتا ہے۔ اس اثر کا اندازہ لگانے کے لئے گوگل کی سکیوریٹی محققین نے سام سنگ کے معروف اسمارٹ فون Galaxy 6S Edge میں سکیوریٹی خامیوں کا پتا لگانے کے لئے تجربات کئے۔ تجربات کا نتیجہ کافی مایوس کن رہا کیونکہ سکیوریٹی ٹیم کو اس فون میں نصب اینڈ رویئڈ میں درجن بھر سکیوریٹی بگ ملے۔

محققین کو مجموعی طور پر گیارہ سکیوریٹی خامیاں ملیں جو سام سنگ کی جانب سے اینڈ رویئڈ میں کی جانے والی تبدیلیوں کی وجہ سے پیدا ہوئیں۔ ان خامیوں کا فائدہ اٹھا کر ہیکر صارف کی ای میل پیغامات چرا سکتا ہے، آپریٹنگ سسٹم کی کرنل میں کوئی کوڈ ایگزی کیوٹ کر سکتا ہے یا کسی ایپلی کیشن کو حاصل حقوق میں اضافہ کر سکتا ہے۔ ٹیم کے مطابق انہیں ملنے والے بیشتر سکیوریٹی بگ انتہائی خطرناک نوعیت کے تھے۔ سب سے زیادہ کمزوریاں ڈیوائس ڈرائیورز اور میڈیا پروسیسنگ کے کوڈ میں دیکھیں گئیں اور ان خامیوں کو تلاش کرنے میں ٹیم کو زیادہ جدوجہد بھی نہیں کرنی پڑی۔ سام سنگ کی مذکورہ ڈیوائس میں ایک خامی path traversal بھی دیکھی گئی۔ سام سنگ کی اپنی ایک سروس جس کا نام WifiHs20UtilityService ہے، سسٹم سروس کے حقوق کے ساتھ ڈیوائس میں چل رہی ہوتی ہے۔ یہ سروس ایک مخصوص جگہ (پاتھ) پر زِپ فائل تلاش کرتی رہتی ہے۔ جیسے ہی اسے وہاں کوئی زِپ فائل ملتی ہے، یہ اسے Unzip کر دیتی ہے۔

اینڈ رویئڈ میں SELinux نامی دفاعی نظام موجود ہوتا ہے جو اینڈ رویئڈ پر حملوں کو ناکام بناتا ہے۔ لیکن سام سنگ کے کوڈ میں ایسی خامیاں بھی ملیں جن کی وجہ سے اس دفاعی نظام کو غیر فعال کرنا ممکن تھا۔ لہٰذا عملی طور پر اس دفاعی نظام کا بھی فائدہ نہ رہا۔

ایسا نہیں کہ اینڈ رویئڈ بذات خود خامیوں سے پاک ہے۔ اینڈ رویئڈ کے خالص کوڈ میں بھی سکیوریٹی ماہرین کامیابی سے خامیاں تلاش کرتے رہتے ہیں۔ ایسی خامیوں کو دور کرنا خاصا آسان ہوتا ہے۔ لیکن ہر موبائل فون مینوفیکچر کی جانب سے اینڈ رویئڈ میں تبدیلیوں کے بعد یہ خامیاں دوچند ہو جاتی ہیں۔ بعض مینوفیکچر اپنی پیدا کردہ خامیوں کو دور کرنے میں حد درجہ سستی کا مظاہرہ کرتے ہیں جو اینڈ رویئڈ آپریٹنگ سسٹم کی شہرت پر اثر انداز ہو رہی ہے۔

ای میل کا کیا جواب لکھیں؟ اب گوگل خود بتائے گا

ہر ای میل کا جواب دینا ضروری نہیں ہوتا۔ لیکن بعض ای میل پیغامات ایسے ہوتے ہیں جن کے جواب دینا ضروری تو ہوتا ہے لیکن یہ ضروری نہیں ہوتا ہے کہ آپ اس کا مفصل جواب لکھیں۔ لوگوں کی مشکل کو آسان کرنے کے لئے گوگل نے مشین لرننگ کا سہارا لیا ہے۔ کمپنی نے اپنے Inbox ای میل کلائنٹ میں ایک نئے فیچر Smart Replies کا اضافہ کیا ہے۔ یہ فیچر موصول ہونے والی ای میل کے مواد کا جائزہ لیتا ہے اور اس کے تین ممکنہ جوابات تیار کر کے استعمال کنندہ کو دکھاتا ہے۔ صارف اگر چاہے تو انہی جوابات میں سے کوئی ایک بھجوا دے یا چاہے تو ان میں سے کسی ایک میں کمی بیشی کر کے بھجوا دے۔ یہ فیچر موبائل فون صارفین کا بہت سے وقت بچا سکتا ہے جنہیں کسی ای میل کا جواب دینے کے لئے موبائل فون پر ٹائپ کرنے کی کٹھن مشقت کرنی پڑتی ہے۔

چونکہ Smart Replies کی بنیاد مشین لرننگ سسٹم ہے اس لئے اسمارٹ ریپلائیز وقت کے ساتھ ساتھ بہتر سے بہترین ہوتا چلا جائے گا۔



ترجمہ و تلخیص: عمیر عادل

نقل کے شاطر ذہنوں اور آئی ٹی سرٹیفکیشنز کے نگراں اداروں کی دلچسپ رسّہ کشی

نقل کے لیے عقل کی ضرورت ہوتی ہے۔لیکن نقل اگر آئی ٹی پروفیشنل سرٹیفکیشن جیسے امتحان کی ہوتو یہاں عقل والے نقل کرنے کے لیے ایسی 'جگاڑیں' کھوجتے نظر آتے ہیں جن کو سمجھنے اور روکنے کے لیے نگراں اداروں کے دانتوں تلے پسینہ آجاتا ہے۔امتحانات چاہے اسکول کے ہوں یا یونیورسٹی کے، ان میں نقل، دھوکا دہی اور جعلی ڈگری کا حصول ایسے 'کارنامے' ہیں جنھیں پاکستان میں رائے عامہ کے مطابق 'قومی کھیل' خیال کیا جاتا ہے۔تاہم حقیقت میں نقل کا رجحان ہمیشہ سے ہی دنیا بھر کے تعلیمی اداروں کے لیے سردرد رہا ہے۔

پروفیشنل سرٹیفکیشن پروگرام بھی اس وبا سے بچے ہوئے نہیں ہیں۔ملازمت میں ترقی، تنخواہ میں اضافہ اور بہتر ادارے میں ملازمت جیسے محرّکات ان سرٹیفکیشن کے حصول میں نقل اور دھوکا دہی کے رجحانات کو جنم دیتے ہیں۔مثلاً نوّے کی دہائی کے آغاز میں انجینئرز بڑی تعداد میں سرٹیفائیڈ نیٹ ویئر انجینئر سرٹیفکیشن حاصل کرتے تھے۔اس سرٹیفکیشن کے حامل افراد کو ملازمت بھی اچھی ملتی تھی اور تنخواہ بھی۔ذرا عرصے بعد ہی انجینئرنگ کے حلقوں اور متعلقہ صنعتوں میں ان سرٹیفائیڈ پروفیشنلز کے معیار کے بارے میں تشویش پیدا ہوگئی اور ایک اصطلاح 'پیپر سرٹیفائیڈ نیٹ ویئر/نویل انجینئر' نے جنم لیا۔یہ وہ انجینئر تھے جنھوں نے پیپر کسی بھی طرح کامیابی سے پاس کرکے سند تو حاصل کرلی لیکن ان کے پاس کام کرنے کا تجربہ تھا نہ سلیقہ۔اس سرٹیفکیشن پروگرام میں دھوکا دہی کے رجحان نے بالآخر اس سند کے معیار اور اعتبار کو ختم ہی کردیا۔

ہر سال ہزاروں لاکھوں لوگ مائیکروسافٹ، سسکو، اوریکل اور دیگر انفارمیشن ٹیکنالوجی سے وابستہ کمپنیوں کی مصنوعات میں اپنی مہارت ثابت کرنے کے لئے امتحانات دیتے ہیں۔آئی ٹی سرٹیفکیشن پروگراموں کو بھی انہی مسائل کا سامنا کرنا پڑتا ہے جو کسی عام ڈگری اور سرٹیفکیٹ پروگرام کو درپیش ہوتے ہیں۔تاہم یہ پروگرام فراہم کرنے والے اور امتحانی مراکز میں نگرانی کرنے والے ان سرٹیفکیشنز کی ساکھ بحال رکھنے کے لیے نقل اور دھوکا دہی کے رجحانات کے خلاف برسرِ پیکار نظر آتے ہیں۔ان کو درپیش سب سے اہم چیلنج، نقل اور دھوکا دہی کے ذریعے سرٹیفکیشن حاصل کرنے کے ان تمام ذرائع اور نت نئے طریقوں کو روکنا ہے جو لوگ استعمال کرسکتے ہیں۔مثلاً لوگ امتحانی مراکز میں بلیوٹوتھ ایئرپیس اور اعلیٰ ٹیکنالوجی کا جاسوس کیمرہ لے کر آسکتے ہیں اس سے وہ ویڈیو کال پر موجود اس کورس کے ماہر کو سوال دِکھا کر جواب سن سکتے ہیں۔'Brain Dump' سائٹس سے چوری شدہ مواد خرید کر سوال و جواب یاد کرسکتے ہیں یا آن لائن چیٹ رومز میں سوال و جواب شیئر کرسکتے ہیں۔اسی طرح سرٹیفکیشن کے خواہش مند لوگ خود پیپر دینے کے بجائے کسی ماہر کی خدمات حاصل کرسکتے ہیں جو ان کی جگہ خود جا کر ٹیسٹ دے سکتا ہے۔اس کے علاوہ موقع پا کر چپکے سے اسمارٹ فون کا استعمال کرنا مثلاً ایس ایم ایس کرنا یا سوالات کی تصویر اُتار کر بھیجنا یا آن لائن سرچ کرنا وغیرہ۔لوگ پرانے نسخے بھی استعمال کرسکتے ہیں مثلاً کارتوس، بُوٹی، پھرّے یا ہتھیلی پر جوابات یا فارمولے وغیرہ لکھنا وغیرہ۔

ایک حالیہ سروے رپورٹ کے مطابق آئی ٹی سرٹیفکیشن تنخواہ میں اضافے اور کیریئر میں ترقی کے لیے بنیادی ذریعہ بن چکی ہے۔لہٰذا سرٹیفکیشن کی مقبولیت بڑھنے کے ساتھ ساتھ نقل اور جعل سازی بھی بڑھ چکی ہے۔جہاں نوکریوں اور تنخواہوں کو خطرات لاحق ہوں وہاں لوگ انہیں بچانے کے لئے ہر قسم کے طریقے استعمال کرنے کی کوشش کرتے ہیں۔

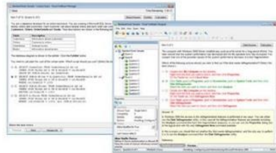
Pearson VUE ایک ادارہ ہے جو مختلف سرٹیفکیشن جن میں آئی ٹی کے پروگرام بھی شامل ہیں، کے لیے دنیا بھر کے پانچ ہزار سے زائد امتحانی مراکز کا

انتظام اور نگرانی کرتا ہے۔ یہ ادارہ دیگر کئی اداروں سمیت CompTIA آئی ٹی سرٹیفکیشن پروگرام کے ٹیسٹ کا انتظام بھی کرتا ہے۔ CompTIA کے اندازے کے مطابق آئی ٹی سرٹیفکیشن امتحانوں میں نقل و فریب کی سطح پانچ فی صد سے کم ہے۔ پھر بھی صنعت کے اندر کے افراد کہتے ہیں کہ یہ مسئلہ بڑھ رہا ہے اور یہ کہ نا صرف آئی ٹی کی صنعت کو بلکہ سرٹیفکیشن فراہم کرنے والے اور نگرانی کرنے والوں کو مستقل ہوشیار رہنے کی ضرورت ہے۔ تاہم اب تک اس رجحان نے آئی ٹی سرٹیفکیشن کو صنعت اور نوکری کے حصول کے لئے بے قدر نہیں کیا ہے۔ فوٹی پارٹنر کی رپورٹ کے مطابق اب بھی سرٹیفکیشن رکھنے والے افراد کی اوسط تنخواہوں میں اضافہ ہوتا ہے۔

تاہم اس حوالے سے یہ جاننے کا کوئی طریقہ نہیں ہے کہ ملازمت پر رکھے جانے والے شخص نے آئی ٹی سرٹیفکیشن حاصل کرنے کے لئے کوئی غلط طریقہ استعمال کیا ہے یا نہیں۔ اسی لیے سرٹیفکیشن کے نگراں اداروں کی طرف سے 'بھروسہ کرو لیکن تصدیق کرو' کے مصداق یہ تجویز دی جا رہی ہے کہ مکمل اطمینان کے لئے ملازمت دینے والوں کو سرٹیفکیشن کے ادارے سے رابطہ رکھنا چاہیے۔ Caveon LLC ایک مشاورتی (کنسلٹینسی) کمپنی ہے جو ڈیٹا فورینسک کے ساتھ ٹیسٹ کی نگرانی میں مہارت رکھتی ہے۔ اس کے نائب صدر کا کہنا ہے کہ ملازمت پر رکھنے والی کمپنیاں زیادہ تر بھروسہ کرسکتی ہیں کہ تصدیق شدہ آئی ٹی سرٹیفکیشن قانونی طور پر حاصل کی گئی ہے۔ محض چند گندے انڈوں نے آئی ٹی پیشے کے افراد کی قابلیت کو مشتبہ بنا ڈالا ہے۔ اسی لیے احتیاط کے طور پر آئی ٹی سرٹیفکیشن کسی شخص کو ملازمت پر رکھنے کے فیصلے کا صرف ایک حصّہ ہونا چاہیے۔ اس کے ساتھ قابلیت کی تصدیق کے لیے مزید اقدامات بھی ہونے چاہئیں مثلاً دیے گئے شخصی حوالوں کی جانچ، سابقہ ملازمتوں کے ریکارڈ کی تحقیقات اور کچھ محتاط سوالات پوچھنا جو یہ اندازہ لگانے کے لیے ترتیب دیئے گئے ہوں کہ اُمیدوار واقعی اپنے شعبے کے متعلق علم رکھتا ہے کہ نہیں۔

مائیکروسافٹ اور CompTIA جیسی آئی ٹی سرٹیفکیشن پروگرامز تشکیل دینے والی کمپنیاں پرومیٹرک (Prometric) اور Preason VUE جیسے ٹیسٹنگ سینٹرز سے معاہدہ کرتی ہیں۔ یہ سینٹرز بالکل ویسے ہی کام کرتے ہیں جیسے پاکستان میں نیشنل ٹیسٹنگ سینٹر (NTS) کا ادارہ کام کرتا ہے۔ یہ ٹیسٹ سینٹرز آئی ٹی کمپنیوں کی جانب سے دنیا بھر میں ٹیسٹ کا انتظام اور نگرانی کرتے ہیں۔ یہ سینٹرز ٹریننگ کی خدمات بھی فراہم کرتے ہیں لیکن یہ ٹیسٹنگ سینٹر ٹریننگ اور ٹیسٹنگ کے کاروبار کے درمیان ایک دیوار قائم رکھتے ہیں تاکہ ایسا محسوس نہ ہو کہ ان کے ٹیسٹنگ سینٹر میں تعلیم حاصل کرنے والے کو دیگر اداروں سے تربیت لینے والوں پر کسی قسم کی سبقت حاصل ہوتی ہے۔

آئی ٹی سرٹیفکیشن فراہم کرنے والے ادارے اپنی گرتی ہوئی ساکھ سے پریشان ہیں۔ اس لیے وہ اپنے ٹیسٹ ڈیٹا کی پائریسی کو روکنے اور نقل کرنے والوں کو پکڑنے کے لیے مزید بہتر طریقے اپنانے کی کوشش کررہے ہیں۔ دوسری جانب نقل کرنے والے ہر وہ طریقہ اپنانے کی کوشش کرتے ہیں جن سے وہ فائدہ اُٹھا سکتے ہوں۔ ایک طریقے میں یہ دیکھا گیا کہ امیدواروں کا ایک گروپ باقی امیدواروں سے واضح سبقت لیتا رہا ہے۔ ایسے امیدوار اپنی جگہ ٹس سے مس نہیں ہوتے اور بمشکل حرکت کرتے تھے۔ وہ ایک سے دو سوال فی منٹ کی عمومی رفتار سے کہیں تیز چھ سوال فی منٹ کی رفتار سے حل کرتے تھے اور ان کے حاصل کردہ نمبر کافی زیادہ ہوتے ہیں۔ CaveonLLC کی تحقیق و تفتیش کے مطابق امیدوار گویا ویڈیو کیمرہ اور بلیوٹوتھ استعمال کرتے ہوئے کال پر مضمون کے ماہر سے رابطے میں ہیں۔ یہ آلات spycheatstuff.com جیسی آن لائن ویب سائٹس سے با آسانی دستیاب ہوتے ہیں۔ نقل کرنے والے امیدوار یہاں سے لاسلکی (وائرلیس) اسپیکر خرید سکتے ہیں جو ان کے کان کے کافی اندر فٹ ہوسکتے ہیں جہاں سے وہ آسانی سے نظر نہیں آتے۔ اس کے علاوہ ننھے خفیف سے جاسوسی کیمرے بھی خریدے جاسکتے ہیں جو آسانی سے چھپائے جا























برین ڈمپس ویب سائٹس نے آئی ٹی سرٹیفکیشنز کی ساکھ کو بری طرح سے متاثر کیا ہے۔ بدقسمتی سے ان ویب سائٹس سے تیاری کرنے والے بڑی تعداد میں اپنا امتحان کامیابی سے پاس کرلیتے ہیں

سکیں۔ ایسی صورتِ حال میں نقل کرنے والے ہر ممکن حد تک کوشش کرتے ہیں کہ وہ ساکت بیٹھے رہیں تاکہ اپنے کیمرے کو پرچے کا صاف منظر دے سکیں۔

جو لوگ ٹیسٹ میں پکڑے نہیں جاتے انہیں تب بھی فکر مند ہونے کی ضرورت ہے۔ PearsonVUE ہر ٹیسٹ کا ڈیجیٹل ویڈیو ریکارڈ رکھتا ہے اور اسے اپنی تحقیقات میں استعمال کرتا ہے۔ ایک کیس میں ادارے کی اسکروٹنی ٹیم نے نوٹ کیا کہ ایک امیدوار اپنے سر کو غیر معمولی انداز میں حرکت دے رہا تھا۔ مزید تفتیش پر معلوم ہوا کہ اس نے اپنی عینک میں کیمرہ چھپایا ہوا تھا۔

مائیکروسافٹ کا کہنا ہے کہ لوگوں کے نقل کرنے کا انداز بدل رہے ہیں اور وہ زیادہ ٹیکنالوجی استعمال کرنے لگے ہیں۔ لیکن سب سے عام طریقے جس کے ذریعے لوگ نقل کرنے کی کوشش کرتے ہیں، وہ زیادہ اعلیٰ ٹیکنالوجی کے حامل نہیں ہوتے۔ زیادہ تر رجحان اب غیر فعال نقل کے طریقوں کی طرف منتقل ہو گیا ہے۔ جیسے برین ڈمپ ویب سائٹس کا استعمال یا پراکسی ٹیسٹنگ سروسز کی مدد لینا وغیرہ۔ مائیکروسافٹ ایسے امیدواروں کو پکڑ چکا ہے جو ان ویب سائٹس پر سوال و جواب پوسٹ کر رہے تھے یا خرید رہے تھے۔ اسی طرح ایسے امیدوار بھی پکڑے جا چکے ہیں جو روایتی طریقے استعمال کر رہے تھے جیسے امتحان میں دوسرے لوگوں کی نقل کرنا، فون کا استعمال کرتے ہوئے میسج کرنا اور حتیٰ کہ کسی اور کی اسکور رپورٹ کو تبدیل کر کے اپنا نام لکھنا وغیرہ۔

برین ڈمپ ویب سائٹس محض ایک جگہ ہی فراہم نہیں کرتیں جہاں صارفین ایک دوسرے سے ٹیسٹ کے سوالات و جوابات کا تبادلہ کرتے ہیں، یہ ویب سائٹس کھلے عام عام ٹیسٹ کا چوری شدہ مواد فروخت کرتی ہیں اور اسے ٹیسٹ کی تیاری کے مواد کے طور پر پیش کرتی ہیں۔ یہ خریداروں کو اس بات کی گارنٹی دیتی ہیں کہ وہ امتحان میں با آسانی پاس ہو جائیں گے۔

برین ڈمپس ویب سائٹس آئی ٹی سرٹیفکیشن پروگرامز کے لئے کسی زہر جیسی ثابت ہو رہی ہیں۔ ان کی مثال ہمارے یہاں امتحانات کی تیاری کے لئے دستیاب Guess Papers یا فائیو ایئرز (جن میں گزشتہ پانچ سالوں کے دوران امتحانی پرچوں میں آنے والے سوالات اور ان کے جوابات موجود ہوتے ہیں) جیسی ہے۔ ان کے ذریعے تیاری کرنے والے اکثر طلبہ امتیازی نہ سہی لیکن پاس ہو ہی جاتے ہیں۔ برین ڈمپس ویب سائٹس میں سے بیشتر براعظم ایشیاء میں یا ایسے ممالک (مثلاً یوکرین) سے چلائی جا رہی ہیں جہاں انہیں بند کرنا اور ان کے مالکان کو سزا دلوانا بہت مشکل ہے۔ کچھ ممالک میں ایسی ویب ہوسٹنگ با آسانی خریدی جا سکتی ہے جس پر ہر قسم کا غیر قانونی مواد شائع کیا جا سکتا ہے اور ہوسٹنگ کمپنی خریدار کی معلومات بھی طلب نہیں کرتی۔ ایشیا میں قائم بعض ٹیسٹنگ سینٹروں میں زیادہ سختی نہیں ہوتی اور وہاں سے امتحان کے سوالات اور دیگر مواد چوری یا نقل کیا جا سکتا ہے۔

برین ڈمپس ویب سائٹس کے مالکان یا درست الفاظ میں 'قزاق' امتحانی سوالات اور ان میں شامل تصاویر وغیرہ چوری کرنے کے لئے مختلف طریقے اپناتے ہیں۔ ان میں سب سے عام طریقہ مخصوص ٹیسٹنگ سینٹروں میں اپنے بندوں کو امتحان دلوانا ہے جو امتحان کے دوران آنے والے سوالات اور ان کے ممکنہ جوابات کو یاد کرتے ہیں یا ان کی تصاویر لیتے ہیں۔ کسی امتحان میں آنے والے سوالات کا ایک ڈیٹا بیس بنانے کے لئے انہیں درجن بھر لوگوں کو ٹیسٹ دلوانا ہوتا ہے۔

بدعنوان یا ایسے مراکز جہاں زیادہ سختی نہ ہوتی ہو وہاں سے ٹیسٹ ڈیٹا کی چوری نسبتاً آسان ہوتی ہے۔ چوں کہ تمام ٹیسٹ اور ان کی جوابی کاپیاں ہر امتحانی مرکز کے سرورز پر ڈاؤن لوڈ ہو جاتی ہیں، اسی لیے وہ ڈیٹا بھی ہیک ہونے کے لئے دستیاب ہوتا ہے۔ یہ تمام باتیں سرٹیفکیشن باڈیز کے لیے بے حد تکلیف دہ رہی ہیں۔ اسی لیے اب سرٹیفکیشن اور امتحان لینے والے ادارے SaaS یا Software as a Service کی طرز پر امتحان کا طریقہ اپنا رہے ہیں۔ اس ضمن میں ایک سرٹیفکیشن سروسز فراہم کرنے والی کمپنی کسی بھی امتحانی مرکز کو بدعنوان یا غیر قانونی سرگرمی میں ملوث پا کر اسے بند کر دیتی ہے۔

کبھی کبھی برین ڈمپ ویب سائٹس استعمال کرنے والا خود بھی دھوکا کھا جاتا ہے۔ یہ ویب سائٹس پیسے

Sure2Pass
Developing Confidence ...
More than 2000 Updated Exams
100% Sure to Pass
Unlimited & Instant Access
Home | Members | All Exams | Microsoft | Support

Free MCSE Braindumps

If you are looking for free mcse braindumps - those are available here. The braindumps for windows 2003 and window 2000 are being displayed as it is as posted by exam takers.

You can share your exam experience and post/send us your exam reviews. The links to mcse braindumps - mcse 2000 braindumps or mcse 2003 braindumps may be posted here, but we are not responsible for the material published on those sites. We invite you to participate to share :

- your experience with MCSE exams
- your favorite MCSE study guides
- MCSE practice exams and
- other mcse braindumps - msca braindumps or mcsd braindumps and resources if you have used.

If you want to post your mcse braindumps - click here

Corrected and verified mcse braindumps enriched with explanations are available in the members area.

Sign up to access the verified and corrected mcse braindumps

All Microsoft Braindumps are available here

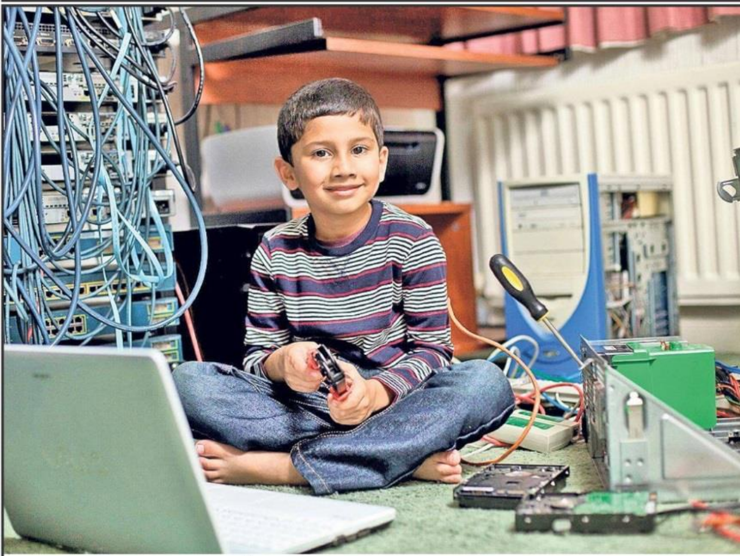
MCSE Hands On Labs
Success Stories about MCSE Braindumps

کئی برین ڈمپس ویب سائٹس سے چوری شدہ مواد صرف قیمتاً ہی نہیں بلکہ مفت بھی دستیاب ہوتا ہے۔ ان میں سے بیشتر ویب سائٹس کی کمائی اپنا سافٹ ویئر بیچنے سے ہوتی ہے جو امتحانات کی تیاری میں معاونت کرتا ہے

لے کر 'بکروں' کو غلط یا تلف شدہ ڈیٹا بھیج دیتی ہیں۔ بعد میں امیدوار لاکھ روتا پیٹتا رہے، اسے اس کی رقم واپس نہیں ملتی۔

آئی ٹی کی صنعت سے وابستہ سبھی ماہر اس رائے سے متفق ہیں کہ لوگ جتنی توانائی اور تخلیقی صلاحیت نقل و فریب کے لیے استعمال کرتے ہیں، اگر یہ مطالعے پر خرچ کریں تو وہ اس سے کہیں بہتر نتائج حاصل کرسکتے ہیں۔

ان قزاقوں کے جواب میں آئی ٹی سرٹیفکیشن باڈیز برین ڈمپ سائٹس، جہاں قزاق چوری شدہ ڈیٹا کو فروخت کرنے کی کوشش کرتے ہیں، پر مربوط حملے کرچکی ہیں۔ جن میں اس جرم کی روک تھام کے احکامات قانون میں شامل ہونا اور پولیس ریڈ بھی شامل ہیں۔ ان آئی ٹی سرٹیفکیشن باڈیز کی کوشش ہے کہ برین ڈمپس ویب سائٹس کو کم سے کم کرنے کے لئے بہترین حکمت عملی اپنائی جائے۔ تاہم ایسا کرنا ناممکن جیسا کام ہے۔ ایک ویب سائٹ بند کرنے سے ویسی ہی درجن بھر نئی ویب سائٹس آن لائن ہوجاتی ہیں۔ ٹورینٹس ویب سائٹس اس کی ایک بڑی مثال ہیں۔ قانون نافذ کرنے والے ادارے آئے دن کسی نہ کسی ٹورینٹ ویب سائٹ کو کاپی رائٹس کی خلاف ورزی کے الزام میں بند کردیتے ہیں، لیکن ٹورینٹس ویب سائٹس کی تعداد گھٹنے کے بجائے بڑھ ہی رہی ہے۔



آیان قریشی نے صرف پانچ سال کی عمر میں مائیکروسافٹ سرٹیفائیڈ پروفیشنل کا امتحان کامیابی سے پاس کرلیا۔ ستمبر 2014ء سے یہ اعزاز انہی کے پاس ہے۔ اتنے کم عمر بچوں کا پروفیشنل امتحان پاس کرلینا ان کی قابلیت کی دلیل تو ہوسکتا ہے، لیکن تصویر کا دوسرا رخ یہ ہے کہ اگر کوئی پروفیشنل امتحان کوئی بچہ اتنی کم عمر میں پاس کرسکتا ہے تو اس سرٹیفکیشن کا معیار کیونکر تسلیم کیا جائے گا؟ کیا اس امتحان کو پاس کرنے کے بعد یہ بچہ کسی ادارے میں وہی کام کرسکتا ہے جو ایک مائیکروسافٹ سرٹیفائیڈ پروفیشنل سے توقع کیا جاتا ہے؟ کیا یہ ممکن ہے کہ کوئی پانچ سال کا بچہ ایم بی بی ایس کا امتحان پاس کرکے ڈاکٹر بن جائے؟

چناں چہ سرٹیفکیشن باڈیز اور نگراں ادارے نقصان کو کم سے کم کرنے کے لیے فوری ردِعمل کرنے کی کوشش کرتے ہیں۔ CompTIA آن لائن برین ڈمپ سائٹس اور چیٹ رومز کو چوری شدہ ٹیسٹ ڈیٹا کے لیے مانیٹر کرتی ہے۔ وہ اس ڈیٹا پر ہونے والی ساز باز پر بھی نظر رکھتی ہے اور کسی گڑبڑ کے نتیجے میں وہ یہ ڈیٹا اُٹھا لیتی ہے۔

زیادہ تر آئی ٹی سرٹیفکیشن امتحان ہر بارہ سے پندرہ مہینوں میں تبدیل کیے جاتے ہیں جبکہ منظّم چوری کے حلقے ٹیسٹ کی پہلی ریلیز کے تین سے پانچ ہفتوں کے اندر اس کی فروخت شروع کردیتے ہیں لہٰذا ان کو روکنے کا عمل کافی مہنگا ہے۔ تاہم CompTIA کے مطابق ڈمپ سائٹس پر سوال ذرا لمبا عرصہ لیتے ہیں اور CompTIA بارہ سے پندرہ مہینوں سے پہلے انہیں تبدیل کردیتا ہے۔

ٹیسٹ ڈیٹا کو جلد تبدیل کرنا بھی ایک بڑا مسئلہ ہے کیوں کہ ٹیسٹ کو تیار کرنے کی قیمت سیکڑوں ڈالر فی سوال سے لے کر ہزاروں ڈالر فی سوال تک ہے۔ لہٰذا بڑے سرٹیفکیشن پروگرام کی بانسبت چھوٹے سرٹیفکیشن پروگرام سوالوں کو تیزی سے تبدیل کرنے میں سستی دِکھاتے ہیں۔ یہی وجہ ہے کہ چھوٹے سرٹیفکیشن پروگرام ہی برین ڈمپس ویب سائٹس سے سب سے زیادہ متاثر ہوتے ہیں۔

ٹیسٹ ڈیٹا چوری کے خطرے کو کم کرنے کے لیے آئی ٹی سرٹیفکیشن فراہم کرنے والوں نے جدید ٹیکنالوجی کا سہارا لینا شروع کردیا ہے۔ اب ٹیسٹ ڈیٹا کو ٹیسٹ دینے والے کے کمپیوٹر تک اِنکرپٹ حالت میں پہنچایا جاتا ہے اور یہ ڈیٹا اسی وقت ڈی کرپٹ کیا جاتا ہے جب ٹیسٹ شروع کیا جاتا ہے۔ ہر امیدوار کے لئے ڈیٹا الگ خفیہ کلید سے اِنکرپٹ کیا جاتا ہے، اس لئے ڈیٹا کی چوری کے امکانات ختم ہوجاتے ہیں۔

CompTIA ٹیسٹ سینٹر کو سوالوں کے جوابات بھی نہیں بھیجتی۔ یہ حل شدہ پرچہ جات واپس لے لیتے ہیں اور آف لائن رہتے ہوئے اس کی اسکورنگ کرکے امیدوار کو نتیجہ بھیج دیتے ہیں۔ اس طریقے سے ٹیسٹ آئٹمز زیادہ عرصے تک چوری سے محفوظ رہتے ہیں۔ تاہم آئی بی ٹی ہمیشہ موزوں نہیں رہتی۔ چونکہ اس کام کے لئے اچھی انٹرنیٹ بینڈ وڈتھ درکار ہوتی ہے، اس لئے کچھ ممالک جہاں



ارفع کریم رندھاوا (مرحوم) نے 2004ء میں صرف نو سال کی عمر میں مائیکروسافٹ سرٹیفائیڈ پروفیشل کا امتحان کامیابی سے پاس کیا۔ یوں یہ دنیا کی کم عمر ترین ایم سی پی بن گئیں اور پاکستان میں انہیں آئی ٹی ماہر کی حیثیت حاصل ہوگئی۔ لیکن درحقیقت اتنی کم عمری میں پروفیشل امتحان کامیابی سے پاس کرنا اس امتحان کے لئے فائدہ مند ہونے کے بجائے نقصان دہ ثابت ہوا کیونکہ اس امتحان کی اہلیت وافادیت مزید مشکوک ہوگئی

قابلِ قبول ہے۔ پراکسی ماہرین امیدوار کی جگہ جاکر ٹیسٹ دیتے ہیں اور اس سے اچھا پیسہ بناتے ہیں۔ کچھ ممالک میں یہ لوگ ایک پراکسی ٹیسٹ دے کر چھ مہینے کی تنخواہ کے برابر رقم کما لیتے ہیں۔

ایشیائی و دیگر ممالک میں جہاں ایسے امتحانی مراکز ہیں جو کسی نہ کسی طرح غیر قانونی کاموں میں ملوث ہیں یہاں پراکسی ٹیسٹنگ سکیوریٹی پروٹوکولز سے کسی طرح بچتی آرہی ہیں۔ یہ امتحانی مراکز قانونی 'فرنٹ روم' یا غیر قانونی 'بیک روم' چلاتے ہیں۔ جب ایک امتحانی مرکز اپنا ذاتی پراکسی حلقہ چلاتا ہے تو ان سخت پروٹوکولز پر عمل درآمد نہیں کیا جاتا جو ان پراکسی کو پکڑنے میں مفید ثابت ہو سکتے ہیں۔ پراکسی ٹیسٹ سے بچنے کے لیے امتحانی مرکز عموماً امیدوار سے تصویری شناخت طلب کرتے ہیں۔ اب کچھ امتحانی مراکز نے بائیومیٹرک شناخت اور ڈیجیٹل دستخط کے ساتھ ساتھ امیدوار کی مرکز کے اندر تصویر بھی کھینچنا شروع کر دی ہے۔ جب ایک بار امیدوار ایک شناخت کے تحت رجسٹرڈ ہو جاتا ہے تو وہ کسی اور کے لیے پراکسی کا کام نہیں کرسکتا۔ مزید یہ کہ جس نے کسی پراکسی کے ذریعے کوئی سرٹیفکیٹ حاصل کیا ہو، اگر وہ دوسرا ٹیسٹ دینے کی کوشش کرے گا تو پکڑا جائے گا کیوں کہ اس کی تصویر اور بائیومیٹرک ڈیٹا ایک جیسا نہیں ہوگا۔ ٹیسٹ سینٹرز میں ٹیسٹ کی چیزوں کو بھی ڈیجیٹل ویڈیو میں ریکارڈ کرسکتے ہیں اور ٹیسٹ دینے والے کی تصویر سرٹیفکیشن رپورٹ میں لگا سکتے ہیں۔ لہٰذا پراکسی ٹیسٹنگ جو کبھی سرٹیفکیشن باڈیز کے لیے سوہانِ روح رہی ہے، ڈیجیٹل فوٹو اور ڈیجیٹل دستخط کی شمولیت سے تقریباً ختم ہوگئی ہے۔

تاہم پراکسی کا مکمل خاتمہ تب ہی ممکن ہے جب ٹیسٹنگ سینٹر معاہدے کی مکمل پاسداری کریں۔ ایسے ٹیسٹنگ سینٹر جو امتحانی خدمات فراہم کرنے والے ادارے (مثلاً PearsonVUE) کی اپنی ملکیت ہوتے ہیں، وہاں پراکسی کے ذریعے امتحان دینا ممکن نہیں۔ لیکن وہ ٹیسٹنگ سینٹر جو ان اداروں سے الحاق شدہ ہوتے ہیں اور ایک معاہدے کے تحت ٹیسٹ لینے کے مجاز بنتے ہیں، میں پراکسی کے خلاف روک تھام کے لئے الحاق شدہ ادارے کی انتظامیہ کی ایمانداری پر بھروسہ کرنا پڑتا ہے اور ایمانداری کو ناپنے کا کوئی آلہ آج تک ایجاد نہیں ہوسکا۔

انٹرنیٹ انفرا اسٹرکچر بہتر نہیں، وہاں اس ٹیکنالوجی کو استعمال نہیں کیا جاسکتا۔

CompTIA جس کی ملکیت میں کئی مشہور آئی ٹی سرٹیفکیشنز ہیں، یہ ادارہ بڑھتے ہوئے پراکسی ٹیسٹنگ سے پریشان ہے۔ زیادہ تر پراکسی کے فراڈ میں امریکا میں موجود امیدوار کا چین میں کسی کو اس مقصد کے لئے کام پر رکھنا ہے۔

چند سال قبل ایک بڑی آئی ٹی سرٹیفکیشن ادارے نے پراکسی کے طریقے کو پکڑنے کے لیے Caveon سے رابطہ کیا۔ یہ سرٹیفکیشن پروگرام Caveon کو معاوضہ دیتے تھے اور وہ اسے ایک پراکسی سروس کو دیتے تھے۔ اس طرح ایک پراکسی سروس کے ذریعے Caveon کے ایک فرد نے یہ اعلیٰ سرٹیفکیشن حاصل کرلی حالاں کہ اس کا اس شعبے میں کوئی تجربہ بھی نہ تھا۔ چند سال قبل پراکسی کی قیمت ایک ہزار ڈالر تھی اور یہ رقم ویسٹرن یونین جیسے ذرائع کے ذریعے بھیجی جاتی تھی۔ اس کی شرائط میں پچاس فیصد ادائیگی امتحان سے پہلے اور پچاس فیصد ادائیگی کام مکمل ہوجانے کے بعد کرنا ہوتی تھی۔ پراکسی ٹیسٹ دینے والی سروسز امریکا سے باہر ایک بڑا کاروبار سمجھا جاتا ہے۔ اس کی ایک وجہ یہ بھی ہے کہ امریکی یہ سمجھتے ہیں کہ نقل وفریب امریکا سے باہر کسی اور جگہ پر روایتی طور پر زیادہ

نقل وفریب کرنے والوں کو پکڑنا خود ایک سائنس بن گیا ہے۔ انٹرنیٹ عام ہونے سے ماضی کے مقابلے میں لوگ اب زیادہ معلومات کا تبادلہ کرنے لگے ہیں۔ تاہم مائیکروسافٹ کے مطابق آئی ٹی سرٹیفکیشن باڈیز اور ٹیسٹ سروسز فراہم کرنے والوں کے پاس ڈیٹا چوری کرنے والوں، شیئر کرنے اور استعمال کرنے والوں کی معلومات حاصل کرنے کے ذرائع بھی بڑھے ہیں۔ مائیکروسافٹ ٹیسٹ کے نگران مقرر کرنے کے ساتھ ساتھ آن لائن نگرانی بھی استعمال کرنے لگی ہے جس میں ٹیسٹ دینے والے کی کمپیوٹر اسکرین کی لائیو فیڈ کے ساتھ ویڈیو کیمرے کا استعمال بھی شامل ہے۔ ویڈیو کیمرے کی ریکارڈنگ کے ساتھ ساتھ ویڈیو کی آن لائن نگرانی بھی کی جاتی ہے۔ اس طرح ہر سوال کے لحاظ سے نقل کرنے والوں کی مشکوک سرگرمیوں پر نظر رکھتے ہوئے ایکشن لینا زیادہ آسان ہوتا ہے۔ آن لائن نگرانی کرنے والا بہتر طور پر مشکوک سرگرمیوں کو بھانپ کر ٹیسٹ وہیں ختم کرسکتا ہے۔

ٹیسٹ سینٹرز کے پاس یہ معلوم کرنے کے بھی طریقے ہیں کہ امیدوار نے چیٹ رومز یا برین ڈمپ سائٹس کے حاصل کردہ مواد سے سوال وجواب یاد کیے ہیں یا نہیں۔ ٹیسٹ کو چھاپنے میں خاص حکمتِ عملی کا استعمال کیا جاتا ہے جو خصوصی طور پر نقل کو پکڑنے کے لیے ترتیب دی ہوئی ہوتی ہیں۔ مثلاً نقل کرنے والے ان سوالات کو حل کرنے میں برق رفتاری کا مظاہرہ کرتے ہیں جو ٹیسٹ میں زیادہ عرصے سے ہوتے ہیں جن میں وہ اچھے نمبر لے سکتے ہیں جبکہ نئے سوالات حل کرنے میں ان کی رفتار نسبتاً کافی دھیمی ہوتی ہے اور وہ ان میں کافی خراب نمبر لے سکتے ہیں۔ اسی طرح کچھ آئی ٹی سرٹیفکیشن امتحانات 'ٹروجن ہارس' سوالات کا استعمال کرتے ہوئے جوابی شیٹ میں دانستہ غلط جواب شامل کرتے ہیں۔ یہ سوالات امیدوار کے حاصل کردہ نمبروں میں شامل نہیں ہوتے۔ جب ٹیسٹ دینے والا ایسے سوالات کے جوابات دیتا ہے جن کے غلط جواب درج ہوتے ہیں تو یہ فرض کرلیا جاتا ہے کہ اس نے چوری شدہ معلومات استعمال کی ہے اس طرح اس کا ٹیسٹ خود بہ خود منسوخ کردیا جاتا ہے۔ ٹیسٹ رزلٹ کی فورینسک تجزیئے سے اس غیر فطری عمل کی نشاندہی کے ذریعے نقل کو پکڑنے میں مدد ملتی ہے۔ سرٹیفکیشن پروگرامز اس طرح اور بھی کئی طریقے استعمال کرتے ہیں۔ جیسے امتحانی پرچوں میں سوالات کی ترتیب بدل دینا، MCQs میں جوابات کی ترتیب بدل دینا، مختلف امتحانی پرچہ جات سے سوالات کو اکٹھا کرنا اور ان میں سے منتخب کرکے کئی مختلف ٹیسٹ بنانا اور ایک ہی امتحانی مرکز میں مختلف امیدواروں کو بالکل مختلف ورژن کا ٹیسٹ فراہم کرنا۔ کچھ سرٹیفکیشن ادارے MCQs کی جگہ کارکردگی کی بنیاد والے سوالات شامل کررہے ہیں جنھیں چوری کرکے ذہن نشین کرنا زیادہ مشکل ہوتا ہے۔ اس 'انحصاری آزمائش' میں ہر اگلا سوال امیدوار کے پچھلے دیئے گئے جواب پر منحصر ہوتا ہے۔ جس سے اندازہ ہوجاتا ہے کہ ٹیسٹ دینے والا ٹیسٹ کے مواد کو قبل از جانتا ہے یا نہیں۔ اگر محسوس کیا جائے کہ امیدوار برین ڈمپس سے تیاری کرکے آیا ہے، امتحان ختم ہوجاتا ہے۔ CompTIA کے مطابق یہ امیدوار کو پرکھنے کا زیادہ بہتر طریقہ ہے۔

سرٹیفکیشن ادارے اب ایسے انحصاری آزمائش کے سوالات میں مزید اضافہ کرتے جارہے ہیں جو منظرنامے (سیناریو) پر مبنی ہوں۔ یہ سوالات امیدوار سے مصنوعی ماحول میں خاص کام ادا کرنے کو کہتے ہیں۔ اس قسم کے سوالات چوں کہ یاد کرنا بہت مشکل ہوتے ہیں اسی لیے اس موقع پر امیدوار کو نقل سے زیادہ مطالعہ کرنا آسان لگتا ہے۔ CompTIA کی ان کوششوں کا لُبِ لباب یہ ہے کہ یہ نقل کو مکمل طور پر نہیں روک سکتے اسی لیے یہ ایسے اقدامات کرتے ہیں جن سے مطالعے کے مقابلے میں نقل کرنے میں زیادہ پاپڑ بیلنا پڑتے ہیں۔

نقل کو روکنے کے ان اقدامات کے ساتھ ادارے نقل کرنے والوں کی سزاؤں میں بھی اضافہ کرتے جارہے ہیں۔ مائیکروسافٹ کے سرٹیفکیشن امتحان میں اگر کوئی امیدوار نقل کرتا پکڑا جائے یا دھوکے کا مرتکب قرار پائے تو اس پر مائیکروسافٹ کے ٹیسٹ دینے کی تاحیات پابندی عائد کی جاتی ہے۔ اس کے علاوہ کسی پچھلے کیس کی جانچ پڑتال میں کوئی امیدوار قصوروار قرار پایا گیا تو مائیکروسافٹ اس امیدوار کو بے نقاب کرکے اس کی سرٹیفکیشن منسوخ کردیتی ہے۔ اسی نقشِ قدم پر اب CompTIA بھی چلنے کی کوشش کررہی ہے۔ ان کے امتحان میں اگر کوئی امیدوار چوری کرتے پکڑا جاتا تھا تو وہ اس کا امتحان منسوخ کرکے اس پر ایک مخصوص عرصے کے لیے دوبارہ ٹیسٹ دینے پر پابندی عائد کردیتی ہے۔ CompTIA کا ارادہ مائیکروسافٹ کی طرح تاحیات پابندی عائد کرنے کا ہے۔ اس کے علاوہ چونکہ اکثر آئی ٹی سرٹیفکیشنز کی چند سال بعد تجدید کروانی ہوتی ہے اور اس کے لئے ایک بار پھر امتحان دینا ہوتا ہے۔ مائیکروسافٹ سمیت دیگر تمام اہم آئی ٹی سرٹیفکیشنز کے ساتھ یہی معاملہ ہے۔ چونکہ دھوکہ دہی سے سرٹیفکیٹ حاصل کرنے والوں کو اس پروگرام کے متعلق محدود علم ہوتا ہے، اس لئے وہ سرٹیفکیٹ کی یا تو تجدید کرواتے ہی نہیں یا پھر امتحان میں ناکام ہوجاتے ہیں۔ آئی ٹی ماہرین کے مطابق انھیں حیرت ہوتی ہے کہ لوگ مطالعہ کرنے کے بجائے نقل اور فریب کاری کی تگ ودو میں رہتے ہیں اور بے شمار سنگین خطرات مول لیتے ہیں۔ ایک خالصتاً ایمانداری سے حاصل کی گئی آئی ٹی سرٹیفکیشن عمر بھر کے لیے خالص فائدہ دیتی ہے۔ جبکہ نقل وفریب صرف سرٹیفکیشن کی ساکھ کو ہی نقصان نہیں پہنچاتا بلکہ یہ امیدوار کے مستقبل کو بھی تاریک کرسکتا ہے۔

تحریر: زائرہ راشد

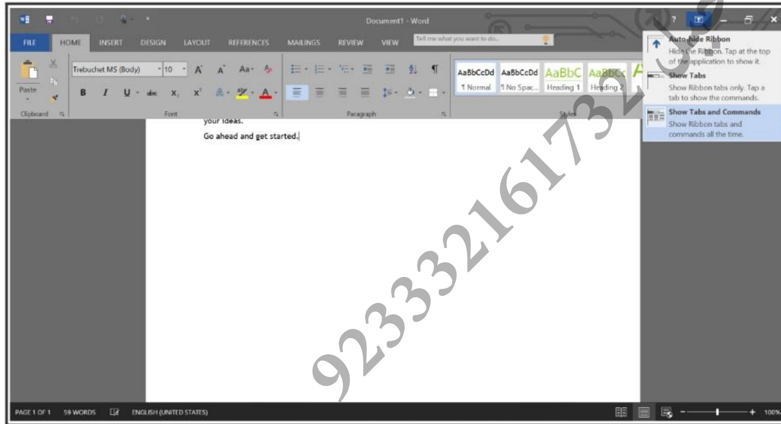
مائیکروسافٹ آفس 2016 کے نئے فیچرز



مائیکروسافٹ کے صارفین کی تعداد بہت زیادہ ہے اس لیے نہ صرف یہ ایک مشہور سافٹ ویئر ہے بلکہ کمپنی کی وسیع آمدنی کا ذریعہ بھی ہے۔ مائیکروسافٹ نے حال ہی میں آفس کا نیا ورژن پیش کیا ہے آفس 2016۔

آفس 2016 ونڈوز اسٹور پر مفت موجود ہے لیکن اس مفت ورژن میں محدود فیچرز ہیں۔ سارے فیچرز تک رسائی حاصل کرنے کے لیے مکمل ورژن ہونا چاہیے۔ اگر آپ office365 کے ساتھ اپنی رکنیت کو برقرار رکھیں تو مفت میں اپ گریڈ حاصل کر سکتے ہیں۔ اس کے علاوہ مائیکروسافٹ کے تمام فیچرز سے فائدہ حاصل کرنے کے لیے مائیکروسافٹ اکاؤنٹ اور ایک ''ون ڈرائیو'' اکاؤنٹ بھی ہونا چاہیے۔

اس نئے ورژن میں کون کون سے نئے فیچرز ہیں، آیئے ان کا جائزہ لیتے ہیں۔



بہتر ڈارک تھیم اور رِبن ٹیب ٹیکسٹ

ان لوگوں کے لیے جو مدھم تھیم کو سخت ناپسند کرتے ہیں ان کے لیے آفس 2016 میں ڈارک تھیم کو بہتر کر کے متعارف کروایا گیا ہے جس کی وجہ سے اس کا اِنٹرفیس استعمال کرنے میں آسان ہو گیا اور ٹیب پر لکھے ہوئے الفاظ با آسانی پڑھے جا سکتے ہیں۔

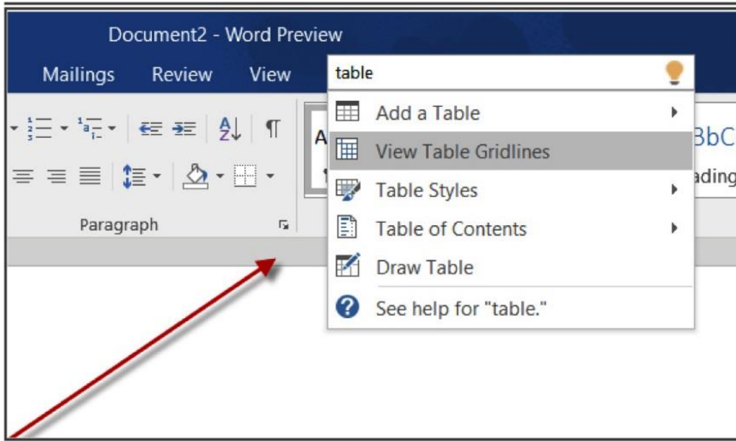
سب سے زیادہ درخواست کیا جانے والا ڈارک تھیم (dark-theme) آپشن آفس 2016 میں موجود ہے۔ صارف اب لائٹ تھیم سے ڈارک گرے تھیم پر منتقل ہو سکتے ہیں۔ ڈارک تھیم منتخب کرنے سے یہ فائدہ ہوتا ہے کہ اگر آپ کی دیر رات تک جاگ کر پڑھنے کی عادت ہے تو اس سے آپ کی آنکھوں پر زور نہیں پڑتا۔

رِبن ٹیب ٹیکسٹ کے الفاظ اب کیپٹل لیٹرز میں نہیں ہیں اور ان پر ماؤس کرسر (cursor) رکھیں تو یہ اپنا رنگ بدلتے ہیں۔

''مجھے بتاؤ'' (Tell me)

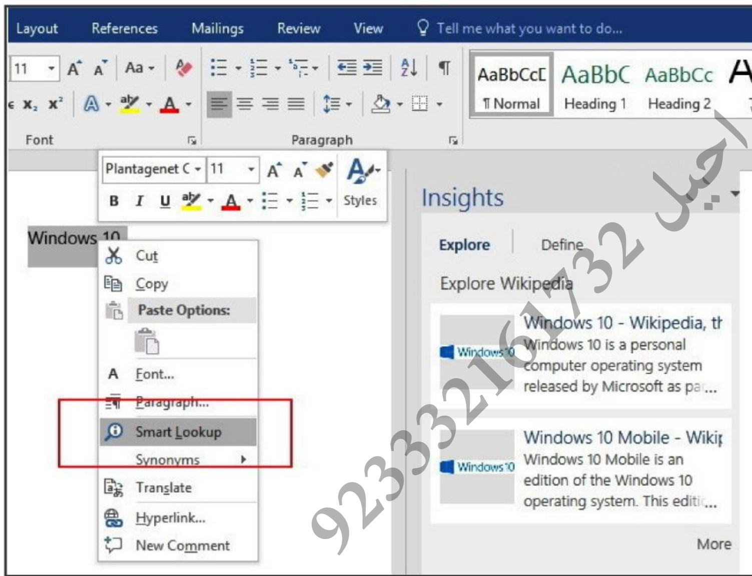
ہم میں سے کافی لوگ آفس کے بہت سے فیچرز اور کمانڈز کو استعمال نہیں کر پاتے کیونکہ ہمیں انہیں ڈھونڈنے میں پریشانی ہوتی ہے۔ اس مسئلے کو حل کرنے کے لیے آفس نے ''ٹیل می'' کا فیچر متعارف کروایا۔ یہ فیچر عام زبان کا استعمال کرتے ہوئے آپشنز ڈھونڈنے میں آپ کی مدد کرتا ہے۔ آفس کی تمام ایپس میں ''ٹیل می'' کا باکس رِبن بار کے ٹیبز کی دائیں جانب ہوتا ہے سوائے پبلشر، ون نوٹ اور اسکائپ کے۔

جب آپ مائیکروسافٹ آفس میں پاور پوائنٹ، ورڈ، ایکسل، ایکسس، آؤٹ لُک اور وزیو وغیرہ استعمال کر رہے ہوں تو جو کام آپ کرنا چاہتے ہیں اسے لِکھ



دیں۔ٹیل می کا آپشن آپ کو اس کام تک لے جائے گا۔یہ ایک ہوشیار معاون کی طرح ہے جو آپ کی باتوں کو آپ کے لکھے ہوئے الفاظ سے سمجھ لیتا ہے۔اس کے علاوہ ایک اور فیچر ہے جو کہ Delve کہلاتا ہے، یہ الگورتھم (Algorithm) کی مدد سے متعلقہ معلومات اور دستاویزات کو ایک جگہ اکٹھا کر دیتا ہے۔

اب جب بھی آپ کو کسی فائل کو اپنے پاس محفوظ کرنا ہو، ایکسل میں گراف بنانا ہو یا آؤٹ لُک میں ای میل میں اپنے دستخط شامل کرنے ہوں، آپ کو صرف یہ کرنا ہے کہ ٹیل می باکس میں آپشن کے بارے میں لکھنا ہے اور یہ آپ کو متعلقہ آپشن تک پہنچا دے گا۔ٹیل می باکس میں کوئی بھی سوال لکھیں، مائیکروسافٹ اس کا سب سے بہترین جواب ڈھونڈ کر لانے کی کوشش کرے گا۔آپ مختلف ویب سائٹس سے معلومات حاصل کرنے کے لیے ''گیٹ ہیلپ'' (Get help) اور اسمارٹ لُک اپ کا بھی استعمال کر سکتے ہیں۔



اسمارٹ لُک اپ

اسمارٹ لُک اپ پہلے ہی ورڈ اور آؤٹ لُک میں دستیاب تھا اور اب اسے ایکسل اور پاور پوائنٹ میں شامل کرلیا گیا ہے۔

اپنی دستاویز میں کسی بھی لفظ کا مطلب جاننے کے لیے اب مائیکروسافٹ کے سرچ انجن بِنگ (Bing) کا فراہم کردہ اسمارٹ لُک اپ استعمال کریں۔صارف اس لفظ کو منتخب کرے جس کا مطلب جاننا چاہتا ہے اور اس پر رائٹ کلک کرتے ہوئے ''اسمارٹ لُک اپ'' پر کلک کرے، اسکرین کے دائیں حصے میں ایک سائیڈ بار کھل جائے گی جس میں منتخب لفظ کے بارے میں مختلف ویب سائٹس سے لی گئی تفصیلات یا معلومات دِکھ رہی ہوگی۔یہ معلومات مختلف ذرائع سے حاصل کی جاتی ہے جیسے کہ وکی پیڈیا آکسفورڈ ڈکشنری وغیرہ سے۔یعنی آپ کو آفس ایپ پر رہتے ہوئے ہی چھوٹی سے بڑی معلومات مل جاتی ہے۔

ایکسل میں اسمارٹ لُک اپ کو نمبرز اور اکویشنز کے بارے میں جاننے کے لیے استعمال کیا جا سکتا ہے۔ایکسل میں موجود فارمولے اور اکویشنز کو بہتر طریقے سے سمجھنے میں بھی یہ مددگار ثابت ہوگا۔

آسان شیئرنگ

آفس کی دستاویز کو شیئر کرنا اب نہایت ہی آسان ہے۔رِبن میں موجود بٹن پر کِلک کریں اور منتخب کردہ لوگوں کے ساتھ اپنی دستاویز کو شیئر کریں۔

کسی بھی دستاویز کو لوگوں کے ساتھ شیئر کرنے کے لیے ''شیئر بٹن'' کا استعمال کریں جو کہ رِبن بار کے اوپری دائیں کونے میں موجود ہوتا ہے۔شیئر کا آپشن استعمال کرنے سے دستاویز ون ڈرائیو اکاؤنٹ کے فولڈر میں محفوظ ہوجاتی ہے۔اپنی دستاویز کو شیئر کرنے سے پہلے اس بات کی یقین دہانی کرلیں کہ آپ نے ون ڈرائیو میں

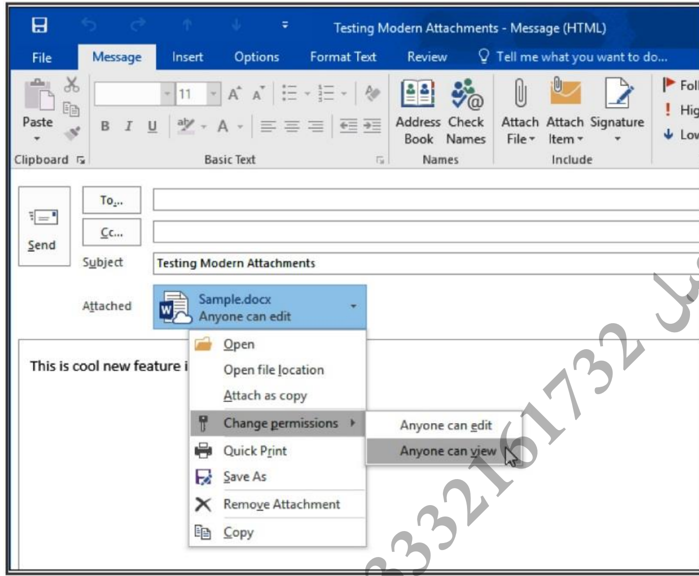
شیئرفولڈر بنایا ہوا ہے۔ آپ اپنی دستاویز میں ہونے والی تبدیلیوں کو فوراً ہوتا ہوا دیکھ سکتے ہیں اور یہ بھی دیکھا جاسکتا ہے کہ کون اس میں تبدیلیاں کر رہا ہے۔

بہتر ورژن ہسٹری

اب آپ پاور پوائنٹ، ورڈ اور ایکسل میں سابقہ اِسنیپ شاٹ (Snapshot) اور پرانی دستاویزات کو دیکھ سکتے ہیں اور ان میں اپنی مرضی کے مطابق تبدیلیاں بھی کرسکتے ہیں۔

میل ٹرائیج (Mail Triage)

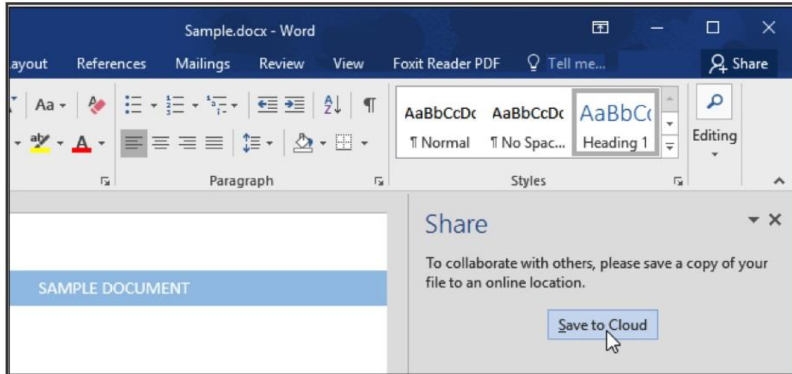
مائیکروسافٹ آؤٹ لُک میں کلٹر (clutter) فیچر یہ پتا لگالیتا ہے کہ آپ ای میلز پر کس سے زیادہ بات کرتے ہیں۔ ان ریکارڈز کا استعمال کرتے ہوئے یہ فیچر آپ کی اہم ای میلز کو ترجیح دیتا ہے اور انھیں آپ کو پہلے دِکھاتا ہے۔ اسی طرح کم ترجیح والی ای میلز کو ایک الگ فولڈر میں ڈال دیتا ہے۔



جدید اٹیچمنٹس

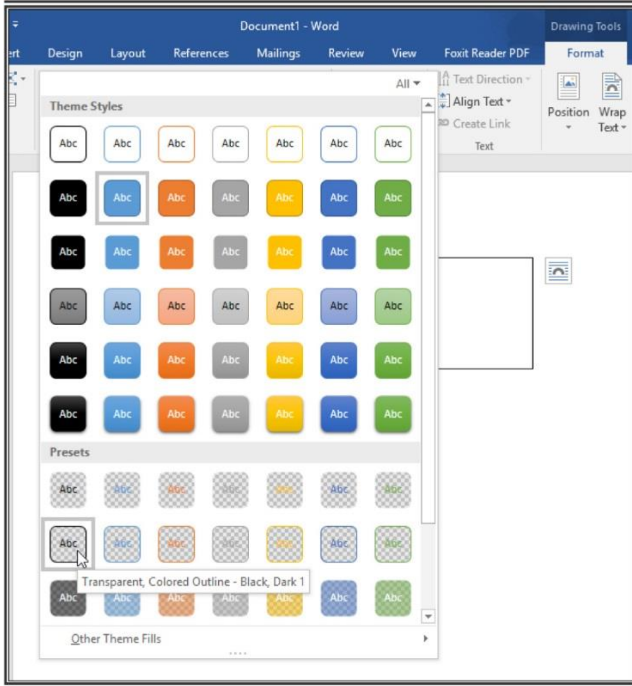
آفس 2016 میں باآسانی کسی بھی دستاویز کو آؤٹ لُک سے منسلک کریں اور ون ڈرائیو یا شیئر پوائنٹ کی مدد سے اپنے کانٹیکٹس کے ساتھ انہیں شیئر کریں۔

آؤٹ لُک 2016 کو بہت پسند کیا جارہا ہے کیونکہ فائلز کو آؤٹ لُک سے منسلک کرنا اب بہت آسان ہوگیا ہے۔ جب آپ ''اٹیچ'' کے بٹن پر کلک کریں گے تو جن فائلز پر حالیہ کام کیا ہے ان کی فہرست سامنے آجائے گی چاہے وہ لوکل فائلز ہوں یا ون ڈرائیو پر موجود ہوں۔ اس سے بہت آسانی ہوجاتی ہے کیونکہ عموماً آپ کو وہی فائل اٹیچ کرنا ہوتی ہے جس پر آپ نے حالیہ کام کیا ہو۔ اگر اٹیچ کی جانے والی فائل حالیہ کام کی ہوئی فائلز کی فہرست میں شامل نہ ہو تو آپ اپنے پی سی سے اس فائل کو منسلک کرسکتے ہیں۔ اٹیچ کی جانے والی فائل کو منتخب کرنے کے بعد فائل کا نام ڈراپ ڈاؤن فہرست بن جاتا ہے جس میں آپشن ہوتے ہیں کہ آپ فائل بھیجنے والے کو فائل سے متعلق کیا اختیارات دینا چاہتے ہیں۔



ٹیم کے ساتھ مل کر کام کریں

گوگل ڈاکس صارفین ریئل ٹائم ڈاکیومنٹ کولیبریشن (Real-time Document Collaboration) کو سالوں سے استعمال کر رہے ہیں تاہم مائیکروسافٹ نے آفس 2016 میں یہ فیچر متعارف کروایا ہے جس کی مدد سے ورڈ، ایکسل اور پاور پوائنٹ میں بنائی گئی دستاویز میں دنیا بھر میں کوئی بھی باآسانی تبدیلیاں کرسکتا ہے چاہے وہ آفس آن لائن استعمال کر رہے ہوں یا ڈیسک ٹاپ آفس ایپ۔



Quick Shape Formatting

اس فیچر کی مدد سے دستاویز میں جب بھی آپ کوئی شیپ بنائیں تو آفس میں فراہم کئے گئے نئے اسٹائل اس پر لاگو کر سکتے ہیں۔

ون ڈرائیو کی شمولیت

ون ڈرائیو کا فیچر آپ کو یہ سہولت فراہم کرتا ہے کہ آفس دستاویز کو کہیں بھی اور کسی بھی ڈیوائس سے استعمال کیا جا سکتا ہے۔ آپ نے آخری بار جہاں کام ختم کیا تھا اگلی بار وہیں سے کام شروع کیا جا سکتا ہے۔

چارٹس کی نئی اِقسام

کسی بھی قسم کے چارٹ پر کام کرنا اور اعداد و شمار کا تجزیہ کرنا اب مشکل نہیں۔ چونکہ مائیکروسافٹ آفس استعمال کرنے والوں کو اکثر اوقات چارٹس بنانے کی ضرورت پڑتی ہے اس لیے آفس 2016 میں چارٹس بنانے کی کئی نئی اقسام شامل کی گئی ہیں۔

بہتر بیک اسٹیج (Improved Backstage)

بیک اسٹیج اسکرین کو اپ ڈیٹ کیا گیا ہے جس کی وجہ سے دستاویز کو محفوظ کرنا، کھولنا اور فائلز کو تلاش کرنے کا عمل آسان اور تیز ہو گیا ہے۔
حالیہ (Recent) فائلز کی فہرست کی ترتیب اب دستاویز کو آخری بار تبدیل کرنے والی تاریخ کے حساب سے ہوتی ہے۔ براؤز (Browse) بٹن فائل ایکسپلورر تک فوری رسائی حاصل کرنے میں مدد کرتا ہے۔

ہاتھ سے لکھی اکویشن کو متن میں بدلیں

ورڈ، ایکسل اور پاور پوائنٹ میں اب ایک نیا فیچر شامل کیا گیا ہے جو ”اِنک اکویشن“ (Ink Equation) کہلاتا ہے۔ اس فیچر کی مدد سے آپ ڈیجیٹل پین، ماؤس یا ٹچ اسکرین ڈیوائسز پر حساب کی اکویشن اپنے ہاتھوں جیسی لکھائی میں لکھ سکتے ہیں۔

اکویشن کو ڈائیلاگ باکس میں لکھیں، آپشنز کا استعمال کرتے ہوئے ٹیکسٹ کو مٹایا جا سکتا ہے، ٹھیک کیا جا سکتا ہے یا اسکرین کو پورا صاف کیا جا سکتا ہے۔ آپ کی ہاتھ سے لکھی ہوئی اکویشن خود بخود ٹائپ شدہ اکویشن میں تبدیل ہو جاتی ہے۔ یہ فیچر اس وقت بہت کام آ سکتا ہے جب آپ کو لمبی اور پیچیدہ اکویشنز لکھنی ہوں یا آپ درست طریقے سے اکویشن ٹائپ نہ کر پا رہے ہوں تو ماؤس سے باآسانی اکویشن لکھ لیں۔

OOO



سوشل میڈیا ہیکرز کی جنت

تحریر: محمد رمیز حنیف

آج کل کے جدید دور میں سوشل میڈیا ہماری زندگیوں کا لازمی حصہ بن چکا ہے۔ پہلے کہتے تھے ”نیکی کر دریا میں ڈال“ اور اب یہ مقولہ بدل کر ”کچھ بھی کر، فیس بک پر ڈال“ بن چکا ہے۔

دکھاوا جو انسان کی فطرت تھا کو سوشل میڈیا نے خوب ہوا دی۔ مسئلہ یہ ہے کہ آپ شیئر کرنا پسند کرتے ہیں، لیکن شاید ضرورت سے زیادہ ہی۔ جی ہاں، آپ کو یہ سکھایا گیا تھا کہ شیئر کرنا اچھی بات ہے لیکن وہ شیئرنگ تھی ”بانٹنا“، کہ سب کچھ اپنے تک محدود نہ رکھیں اس میں دوسروں کو بھی شریک کریں۔ اب اس نئی نسل نے اس شیئرنگ کو سوشل میڈیا پر شیئرنگ کے طور پر لیا۔ خوشی ہو یا غمی ہر موقعے پر سوشل میڈیا پر شیئر کرنا لازم ہو چکا ہے۔

کہتے ہیں کہ سوشل میڈیا پر آپ کی پروفائل جس پر آپ اپنے خیالات کا اظہار کرتے ہیں آپ کی شخصیت کی عکاس ہوتی ہے۔ اگر آپ کسی سے ملے بغیر اس کے بارے میں جاننا چاہتے ہیں تو یہ بہت آسان ہو گیا، آپ کسی کی بھی پروفائل دیکھ کر اندازہ لگا سکتے ہیں کہ وہ کس قسم کے خیالات کا مالک ہے۔

آپ کو پتا ہونا چاہیے کہ ضرورت سے زیادہ شیئرنگ سے پرائیویسی اور سکیورٹی کو خطرات لاحق ہو سکتے ہیں۔ ماہرین کئی سالوں سے نصیحت کر رہے ہیں کہ اس طرح اضافی معلومات کو سوشل میڈیا پر نشر نہ کیا جائے۔ ایسی ان گنت کہانیاں ہیں کہ لوگوں کو فیس بک کی سرگرمیوں کی وجہ سے ملازم کو اضافی فوائد ملنا بند ہو گئے یا نوکری سے ہاتھ دھونا پڑا وغیرہ۔

سوشل میڈیا سے لاحق یہ خطرات صرف مالک، ملازم یا بیمہ کمپنیوں تک محدود نہیں ہیں بلکہ سوشل میڈیا سے معلومات حاصل کر کے جرائم پیشہ افراد پیجز کو اور براہِ راست لوگوں کو اپنا شکار بناتے ہیں اور اپنے فائدے کے لئے اس معلومات کو استعمال کرتے ہیں۔

سب کو اس بات کا احساس کرنا چاہیے کہ ہیکرز آپ کے ذاتی ڈیٹا کے پیچھے پڑے ہوتے ہیں اور ایک دفعہ ان کے ہاتھ یہ ڈیٹا لگ جائے تو پھر وہ اس کا استعمال کیسے کرتے ہیں، اس کا آپ کو اندازہ نہیں۔

مستند معلومات کی چھان بین

جب بھی آپ بینک، ٹیلی کام کمپنی یا گورنمنٹ ایجنسی وغیرہ کی سروسز حاصل کرنے کے لیے سائن اپ کرتے ہیں تو اپنی شناخت کی تصدیق کروانا ضروری ہوتا ہے۔ آن لائن یہ کام یوزرنیم اور پاس ورڈ فراہم کرنے سے ہو جاتا ہے اور کبھی کبھار ایک منفرد کوڈ بذریعہ پیغام صارف کے موبائل پر بھیج دیا جاتا ہے۔

روزمرہ کے معمولات میں مثلاً اگر آپ کو اپنے بینک اکاؤنٹ یا کریڈٹ کارڈ کے بارے میں کچھ تفصیل جاننے کے لیے بینک میں بات کرنی ہو یا اپنی موبائل کمپنی سے رابطہ کر کے اپنا پیکیج بدلنا ہو وغیرہ تو کمپنی یا بینک صارف کی تصدیق کرتا ہے اور اس تصدیقی عمل میں صارف کی تاریخِ پیدائش، شناختی کارڈ نمبر، فون نمبر یا والدہ کا نام وغیرہ پوچھا جاتا ہے۔

کیا آپ کو یہ لگتا ہے کہ ہیکرز کو ان معلومات تک پہنچنے میں مشکل درپیش ہو گی؟ جبکہ آپ سوشل میڈیا پر مستقل اپنی تصاویر، اسٹیٹس اور اپنے بچے کی اگلی سالگرہ کی منصوبہ بندی کو شیئر کرتے ہیں تو بنیادی طور پر آپ اپنی ذاتی معلومات ہیکرز کو پیش کر رہے ہوتے ہیں۔

آپ یہ سوچ رہے ہوں گے کہ شاید والدہ کا نام خفیہ رہے گا۔ شاید نہیں کیونکہ آپ فیملی ممبرز سے آن لائن تعلق میں رہتے ہیں، کبھی ماں سے محبت کا اظہار کرنے کے لیے اس کے ساتھ کھینچی کوئی تصویر بھی شیئر کر دیتے ہیں، اگر آپ نام نہ بھی لکھیں تو کوئی دوست رشتے دار ان کا نام لے کر دعائیں دے دیتا ہے۔ اکثر اوقات تو مائیں بھی سوشل میڈیا پر اکاؤنٹ رکھتی ہیں تو آپ کی والدہ کا نام پتا لگانے میں ہیکر کو کسی مہارت کی بھی ضرورت نہیں۔

اگلی بار جب آپ اپنے بینک یا کسی اور کمپنی میں بذریعہ فون اپنی تصدیق کروا رہے ہوں تو سوچیے گا کہ جو معلومات آپ اس عمل میں اُن کو فراہم کر رہے ہیں کیا

کوئی دوسرا اسے نہیں جانتا یا جان سکتا؟؟

پاس ورڈ کے بارے میں اندازہ لگانا

ہیکرز شاید آپ کے پاس ورڈ کا پتا کرنے کے لیے بہت سے ممکنہ پاس ورڈ لگانے کی کوشش کریں جب تک صحیح پاس ورڈ نہ مل جائے، اس طریقے کو ''بروٹ فورس اٹیک'' کہتے ہیں۔ یہی وجہ ہے کہ صارفین سے مشکل پاس ورڈ رکھنے کا کہا جاتا ہے جس میں اپر کیس، لوئر کیس، نمبر اور خاص کریکٹرز شامل ہوں۔

صحیح پاس ورڈ کو کم وقت میں پتا لگانے کے امکانات کو بڑھانے کے لئے ہیکرز ایک طریقہ استعمال کرتے ہیں جسے ''ڈکشنری اٹیک'' کہتے ہیں۔

ڈکشنری اٹیک کا مطلب یہ نہیں ہے کہ معلومات کے مجموعہ سے ہر ممکنہ بننے والے لفظ کو پاس ورڈ سمجھا جائے بلکہ اس کے برعکس ڈکشنری سے مختلف الفاظ کا استعمال کیا جاتا ہے۔ یہ اٹیک با اثر ہوتا ہے چونکہ بہت سے لوگ بے ترتیب پاس ورڈ کو منتخب نہیں کرتے بلکہ ایسے الفاظ اور ناموں کا استعمال کرتے ہیں جو انھیں با آسانی یاد رہ جائیں۔

Mr.Robot نامی ایک شو میں یہ بتایا گیا تھا کہ سوشل میڈیا پر موجود آپ کی معلومات سے ہیکرز با آسانی بہت سے الفاظ اپنی ڈکشنری میں جمع کرلیتے ہیں جیسے کہ آپ کے فیملی ممبرز یا پالتو جانور کا نام، آپ کی تاریخِ پیدائش یا شادی کی سالگرہ، آپ کے بچے کی تاریخِ پیدائش وغیرہ۔

ان ذاتی معلومات کا استعمال کرتے ہوئے ہیکرز اکثر پاس ورڈ جاننے میں کامیاب ہوجاتے ہیں اور ان کو زیادہ مشقت بھی نہیں ہوتی کیونکہ سارا ڈیٹا تو بذریعہ سوشل میڈیا آپ نے ہی فراہم کیا ہوا ہوتا ہے۔

اداروں پر حملہ بذریعہ ملازمین

ہیکرز محض انفرادی شخص یا پیجز کی ہیکنگ تک ہی خود کو کیوں محدود کرلیں جب بڑے ادارے بھی ہیک ہونے کے لیے تیار ہیں۔

جبکہ کسی ادارے کے اندرونی نیٹ ورک کو ہیک کرنے میں پیچیدگیاں ہوتی ہیں اور بہت مہارت کی بھی ضرورت ہوتی ہے لیکن کسی ادارے کو ہیک کرنے کی جڑ ذاتی ہیکنگ سے مختلف نہیں۔ تنظیموں اور بڑی کمپنیوں کے بھی سوشل میڈیا پیجز ہوتے ہیں جسے وہ مستقل اپ ڈیٹ کرتے رہتے ہیں، وہ بھی ضرورت سے زیادہ شیئرنگ کی وجہ سے نقصان اُٹھاتے ہیں۔

کسی بھی ادارے پر حملہ کرنے کا سب سے عام طریقہ یہ ہے کہ ان کے ملازموں کو ایسی ای میل بھیجی جائیں جن میں مال ویئر ہو۔ ایک بار ملازم اس ای میل کو کھول لے تو اس کمپیوٹر پر مال ویئر حملہ کردیتا ہے جس کی مدد سے ہیکرز ادارے کے اندرونی نیٹ ورک تک پہنچ جاتے ہیں۔ یہ ای میل صرف ان صاحب کے ان باکس تک محدود نہیں رہتی بلکہ ان کے کانٹیکٹ لسٹ میں موجود تمام ای میل ایڈریس پر خود بخود فارورڈ ہوجاتی ہے، اس طرح یہ حملہ مزید خطرناک صورت اختیار کرلیتا ہے۔ آج کل تو کچھ اسمارٹ فون کے مال ویئر بھی فون میں محفوظ تمام نمبرز پر مال ویئر زدہ ویب سائٹس کے لنکس بھیج دیتے ہیں۔

ادارے کے کچھ ملازم دوسروں کے مقابلے میں زیادہ آسان شکار ہوتے ہیں۔ مثال کے طور پر سسٹم ایڈمنسٹریٹر جو پورے آئی ٹی نیٹ ورک کو چلاتے اور سنبھالتے ہیں۔ اگر ان کے کمپیوٹرز مال ویئر سے متاثر ہوجائیں تو یوں کہا جاسکتا ہے کہ ہیکرز کو محل کی چابی مل جاتی ہے اور پورے آئی ٹی انفراسٹرکچر تک رسائی حاصل ہوجاتی ہے۔

اب آپ جان گئے ہوں گے کہ ہیکرز معلومات کو سوشل میڈیا سے حاصل کرتے ہیں۔ سوشل نیٹ ورک سے یہ شناخت کیا جاتا ہے کہ کون سے ملازمین با آسانی نشانہ بن سکتے ہیں یا جس ادارے کو ہدف بنانا ہے اس کے کس ملازم کو نشانہ بنا کر مال ویئر بھیجنا ہے۔ زیادہ تر ادارے مخصوص ای میل ایڈریس اسکیم کا استعمال کرتے ہیں جس میں ملازم کا پہلا نام، فُل اسٹاپ پھر آخری نام آتا ہے تو اگر ہیکر کو ملازم کا نام پتا چل جائے تو اس کے ای میل ایڈریس کا اندازہ لگایا جاسکتا ہے۔ اب جب سبھی نے فیس بک پر اپنا نام اور اپنی کمپنی کا نام لکھا ہوتا ہے تو بھلا ہیکرز کا دل کیوں نہیں للچائے گا۔

سوشل میڈیا ہیکرز کی اس میں بھی مدد کرتا ہے کہ ملازم کو مال ویئر والی جو ای میل بھیجنی ہے اس کا میسج کیا ہونا چاہیے۔ اگر ملازم نے سوشل میڈیا پر یہ پوسٹ کیا ہے کہ وہ کسی کانفرنس میں جارہا ہے تو ہیکرز اپنی ای میل کے میسج کو کانفرنس سے متعلق رکھے گا تاکہ ملازم کسی ہچکچاہٹ کے بغیر اس ای میل کو کھول لے۔

شیئرنگ محدود، پرائیویسی محفوظ

اس طرح کے بہت سے خطرات لاحق ہوسکتے ہیں اگر آپ بغیر سوچے سمجھے سوشل میڈیا پر ضرورت سے زیادہ معلومات شیئر کریں گے۔ ہم نے اس بارے میں تو تفصیل میں بات بھی نہیں کی کہ جب ایک ہیکر نقلی پروفائل بنا کر آپ تک رسائی حاصل کرے تو وہ کیا کچھ کرسکتا ہے۔

اگر اس بات پر غور کیا جائے کہ سوشل میڈیا کس طرح ہماری زندگیوں میں سرایت کرچکا ہے تو عقل مندی اسی میں ہے کہ آپ کو ان خطرات کا علم ہونا چاہیے۔ لہٰذا سوچ سمجھ کر آن لائن شیئرنگ کریں۔

فیس بک کی 15 حیران کن باتیں



سوشل نیٹ ورکنگ کی سب سے مشہور ویب سائٹ فیس بک کی بہت سی حیران کر دینے والی باتیں جو لوگ عموماً نہیں جانتے ہوں گے، آیئے ہر دل عزیز ویب سائٹ فیس بک کے بارے میں ایسی پندرہ دلچسپ باتوں کے بارے میں آپ کو بتاتے ہیں۔



ایل پچینو (AL PACINO) فیس بک کا پہلا چہرہ

یہ ایک نا قابلِ یقین بات ہے کہ فیس بک کا پہلا چہرہ ایل پچینو تھے۔ 2007 تک کچھ وجوہات کی بناء پر لوگ یہ مانتے رہے کہ فیس بک کا پہلا چہرہ مارک زکر برگ (Mark Zuckerberg) تھے۔ چونکہ ایل پچینو کا انتہائی غیر معروف انداز استعمال کیا گیا تھا اس لیے لوگ یہ مانتے رہے کہ فیس بک کا پہلا چہرہ مارک زکر برگ اور اس کے دوست اینڈریو مکولم (Andrew McCollum) نے بنایا ہے۔

فیس بک اکاؤنٹس کو ہیک کرنے کی روزانہ ۶ لاکھ (600,000) کوششیں کی جاتی ہیں

ہیکرز زیادہ تر اپنے ہی احباب اور دوستوں کے اکاؤنٹس ہیک کرتے ہیں تاکہ ان کا غلط استعمال کر سکیں یا پھر وہ اپنے دوستوں کے ساتھ مذاق کرنے اور انہیں تنگ کرنے کے لیے بھی ایسا کرتے ہیں۔

64 فیصد صارف فیس بک کا روزانہ استعمال کرتے ہیں

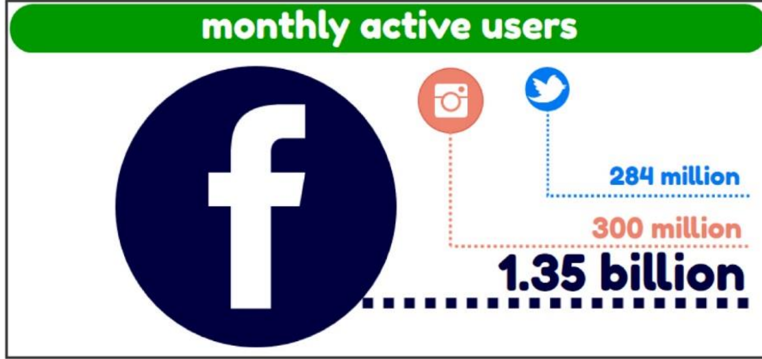
2014 میں منعقد ہونے والی پیو اِسٹڈی (Pew Study) کے مطابق فیس بک کے ایک ارب سے زائد صارفین میں سے 64 فیصد روزانہ فیس بک کا استعمال کرتے ہیں یعنی ایک دن میں 640 ملین (640 million) سے زائد لوگ اپنے فیس بک اکاؤنٹس کا دورہ کرتے ہیں۔

ہر تین طلاقوں میں سے ایک طلاق کی وجہ فیس بک ہے

برٹش لیگل آرگنائزیشن (British Legal Organisation) کی سروس ڈیورس آن لائن (Divorce Online) کے سروے کے مطابق پچھلے

سال ہونے والی تین طلاقوں میں سے ایک طلاق کی وجہ فیس بک تھی۔ اس کی وجہ یہ بتائی گئی کہ سوشل نیٹ ورکنگ دوسروں سے تعلقات بڑھانے میں آسانی فراہم کرتی ہے جس کی وجہ سے آپ کے چاہنے والوں کی تعداد میں اضافہ ہوجاتا ہے۔

ماہانہ ایک ارب سے زائد لوگ فیس بک تک رسائی حاصل کرتے ہیں



دنیا کی آبادی سات ارب لوگوں پر مشتمل ہے جن میں سے ایک ارب لوگ ماہانہ فیس بک استعمال کرتے ہیں۔ فیس بک کے ماہانہ صارفین کی تعداد ایک اعشاریہ پینتیس ارب (1.35 billion) سے زیادہ ہے جو کہ انڈیا کی کُل آبادی سے بھی زیادہ ہے۔

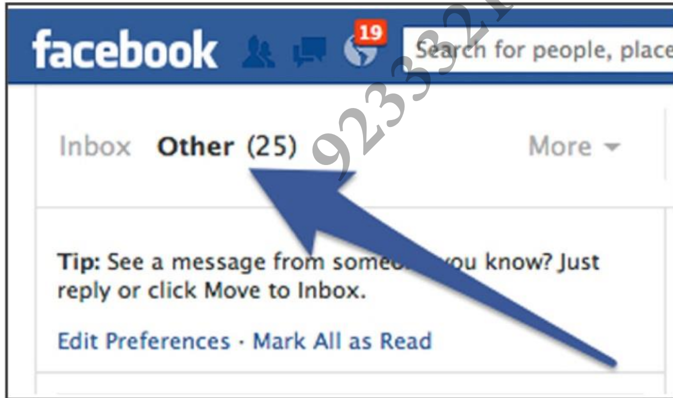
فیس بک پر اَن فرینڈ کرنے کی وجہ سے قتل

ایک شادی شدہ جوڑے نے تیس سالہ خاتون کو فیس بک پر اَن فرینڈ کر دیا تھا جس کی وجہ سے اس خاتون کے باپ نے اُن دونوں کا قتل کر دیا۔

فیس بک صارف کے لاگ آؤٹ ہونے کے باوجود صارف کی وِزٹ کی ہوئی ویب سائٹس کا ریکارڈ رکھتا ہے

2014 میں فیس بک اپنے ویجٹس (Widgets) جیسے کہ لائیک بٹن (Like Button) کا استعمال کرتے ہوئے یہ ریکارڈ رکھنے لگا کہ صارف کون کون سی ویب سائٹس کا دورہ کرتے ہیں۔

پیسے دے کر پیغام کسی کے اِن باکس میں پہنچائیں



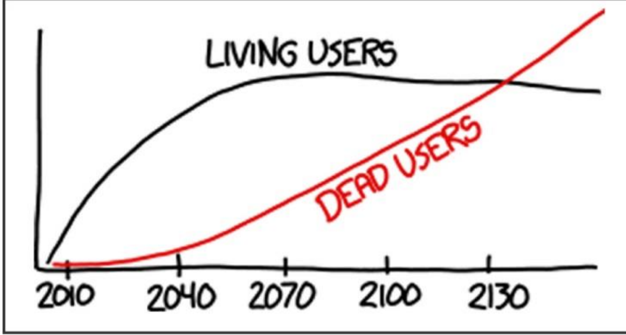
کیا آپ کو پتا ہے کہ جب آپ فیس بک پر کسی ایسے فرد کو پیغام بھیجتے ہیں جو کہ آپ کا دوست نہیں ہے تو ضروری نہیں کہ آپ کا پیغام اس کے ان باکس میں پہنچے، بلکہ فیس بک اپنے صارفین کو پریشانی سے بچانے کے لیے اجنبیوں کے پیغامات کو ان باکس کی بجائے ایک دوسرے فولڈر Other میں منتقل کر دیتا ہے، جسے لوگ شاذ و نادر ہی دیکھتے ہیں۔ لیکن آپ چند پیسے دے کر اپنا پیغام براہِ راست اِن باکس تک پہنچا سکتے ہیں۔ اس سے یہ فائدہ ہوگا کہ آپ کا پیغام Other کے فولڈر میں نہیں جائے گا جس میں آنے والے پیغامات کو کوئی نہیں دیکھتا۔

فیس بک صارف فیس بک استعمال کرنے کے بعد اپنی رائے دے سکتے ہیں

کیا آپ نے کبھی فیس بک استعمال کر کے اپنی آرا سے فیس بک کو آگاہ کیا ہے؟ یہ حیران کر دینے والی بات ہے کہ ایک اندازے کے مطابق تین صارفین میں سے ایک صارف نے یہ کہا کہ انہیں فیس بک کا دورہ کرنے کے بعد بہت بُرا احساس ہوا۔

کیا آپ جانتے ہیں کہ فیس بک کا رنگ نیلا کیوں ہے؟

مارک زکر برگ کو ریڈ گرین کلر بلائنڈ نیس (Red-Green Color Blindness) کا مرض ہے اسی لیے اس نے فیس بک کے لیے نیلے رنگ کا انتخاب کیا۔ مارک زکر برگ نے 2010 میں نیو یارک کے رپورٹر Jose Antonio Vargas کو بتایا کہ نیلا رنگ ان کے لیے خاص ہے کیونکہ وہ نیلے رنگ جیسے ہر رنگ کو بخوبی دیکھ سکتے ہیں۔



ایک دن ایسا آئے گا جب فیس بک پر مُردہ لوگوں کی تعداد زندہ لوگوں سے زیادہ ہوگی

فیس بک کے صارفین میں دن بدِن اضافہ ہو رہا ہے جس کی وجہ سے 2060 یا 2130 میں ایک وقت ایسا آئے گا جب فیس بک کے وہ صارف جو مر چکے ہوں گے، کی تعداد اُن لوگوں سے زیادہ ہوگی جو اُس زمانے میں فیس بک استعمال کر رہے ہوں گے۔

فیس بک کے URL کے آخر میں 1/4 لگا کر آپ براہِ راست مارک زکر برگ کی wall پر پہنچا دیے جائیں گے

2060 یا 2130 میں کسی وقت، url کے آخر میں 5 یا 6 لگا کر Chris Hughes اور Dustin Moskovitz کی متعلقہ پروفائلز تک جایا جا سکتا ہے جو کہ فیس بک کے شریک بانی ہیں اور فیس بک کے بانی مارک زکر برگ کے کالج کے روم میٹ ہیں۔ اسی طرح سے اگر فیس بک کے url کے آخر میں 7 لگائیں گے تو Arie Hasit کی پروفائل تک رسائی حاصل کر سکتے ہیں جو کہ مارک زکر برگ کے ہارورڈ میں دوست ہوا کرتے تھے۔

طوائفیں بھی فیس بک کا استعمال کرتی ہیں

2011 میں کولمبیا یونیورسٹی کی ایک اِسٹڈی کے مطابق یہ دعویٰ کیا جاتا ہے 83 فیصد طوائفوں نے فیس بک اکاؤنٹ بنائے ہوئے ہیں کیونکہ اس کے ذریعے وہ با آسانی نئے دوست اور گاہک بنا لیتی ہیں۔



بالغ فیس بک صارف کے اوسطً 338 دوست ہوتے ہیں

2014 میں ہونے والی پیو اِسٹڈی کے مطابق فیس بک صارف کے اوسطً 338 دوست ہوتے ہیں۔

پوک (Poke) کا کیا مطلب ہے؟

پوک کا مطلب یا اس کا استعمال فیس بک میں آج تک نامعلوم ہے۔ کیا یہ کسی سے بات شروع کرنے کے لیے ہے یا کسی کو تنگ کرنے کے لیے۔ فیس بک نے سرکاری طور پر اس بات کا جواب کبھی نہیں دیا۔ چونکہ اس کا مقصد واضح نہیں ہے اس لیے لوگ اسے اپنی اپنی سمجھ کے مطابق استعمال کرتے ہیں۔ مثال کے طور پر آپ اس کا استعمال کسی کو یہ بتانے کے لیے کر سکتے ہیں کہ آپ آن لائن ہیں اور جواب ملنے کا انتظار کر رہے ہیں۔















فیس بک پر آنے والے نئے جعلی ڈِس لائیک بٹن کی فراڈ اسکیم

سوشل نیٹ ورکنگ ویب سائٹ فیس بک کے سی ای او مارک زکر برگ نے حال ہی میں لوگوں کو آگاہ کیا تھا کہ کمپنی ایک نئے فیچر (feature) پر کام کر رہی ہے، اس فیچر کہ ذریعے آپ کسی پوسٹ کو ڈِس لائیک کر سکیں گے۔ یہ ڈِس لائیک بٹن دُکھ اور ہمدردی والی پوسٹس جن پر افسوس کا اظہار کرنا چاہیے، اُن پر نامعقول لائیک (like) کرنے سے بچنے کے لیے دیا جا رہا تھا۔ فیس بک پر آنے والے اس نئے فیچر کی خبر نے سائبر کرِمنلز (cybercriminals) کے لیے ممکن کر دیا ہے کہ وہ ویب سائٹ استعمال کرنے والے معصوم لوگوں کو نئے قسم کے فراڈ میں پھنسا سکیں۔

ہیک ریڈ (Hackread) کی رپورٹ کے مطابق ایک پوسٹ فیس بک پر صارفین کو یقین دلاتی ہے کہ وہ دی گئی ویب سائٹ پر جا کر ڈِس لائیک بٹن وقت سے پہلے حاصل کر سکتے ہیں اور اس طرح اُس ویب سائٹ کے وزٹ بڑھ جاتے ہیں۔ اس کے علاوہ یہ پوسٹ بتاتی ہے کہ فی الحال یہ صرف انوائٹ اونلی سِسٹم (invite only system) ہے۔

اس فراڈ اسکیم میں بہت سے لِنکس (links) ہوتے ہیں جن پر کلک کرنے سے صارف بدنیتی پر مبنی نقصان دہ ویب سائٹس پر چلا جاتا ہے جہاں پر ایک کاؤنٹ ڈاؤن ٹائمر (count down timer) ظاہر ہوتا ہے جو صارف کو فوراً دی گئی ریکوائرمینٹس (requirements) کو مقررہ وقت پر بھرنے کے لیے آمادہ کرتا ہے یا پھر ڈِس لائیک بٹن وقت سے پہلے حاصل کرنے کا موقع بھول جانے کے لیے خبردار کرتا ہے۔ اس کے بعد یہ فراڈ اسکیم صارف کو وہ ویب سائٹ فیس بک پر اور میسنجر (messenger) کی کسی بھی پانچ کنورزیشن گروپس (conversation groups) پر شیئر (share) کرنے کے لیے کہتی ہے۔

جب یہ تمام لِنکس پھیلا دیے جائیں گے تب یہ فراڈ اسکیم صارف کو ایک نئے پیج کی طرف راغب کرے گی جہاں صارف کو بہت سارے سرویز (surveys) بھرنے کو کہا جائے گا جس کے ذریعے صارف کی تمام ذاتی معلومات اور اکاؤنٹ معلومات (account credentials) حاصل کر لے گا۔ اس کے بعد مبینہ طور پر اُس صارف اور اس کے روابط کو ای میل (email) کے ذریعے اندھا دھند پیغام بھیجنا شروع ہو جاتے ہیں۔ اس کے علاوہ یہ بات بھی رپورٹ کی گئی ہے کہ اس فراڈ اسکیم میں بہت سی ایسی چیزیں بھی ہیں جو آپ کے کمپیوٹر میں مال ویئر (malware) انسٹال کرنے کی صلاحیت رکھتی ہے۔

Activate newly introduced facebook dislike button on your profile.
And complete the participation requirements
Invitation expires in 362.3 Seconds
Follow these 2 simple steps below to Get Dislike Button
Step 1: Share This Page
Share On Facebook
Step 2:Click On Send Button Below Then Select 5 Groups and hit SEND
Send

یہ بات اب تک نا معلوم ہے کہ کتنے افراد اس آن لائن فراڈ سے متاثر ہوئے ہیں۔ ساتھ ہی فیس بک کے تمام صارفین کے لیے مشورہ ہے کہ کسی بھی مشکوک یا بظاہر بہت اچھی نظر آنے والی کسی بھی پوسٹ پر کلک کرنے سے پہلے دوبار ضرور سوچ لیں۔

فروری میں بھی اسی طرح کا ایک انٹرنیٹ کرائم رپورٹ کیا گیا تھا جس میں مبینہ طور پر ایک ویڈیو صارفین کو goo.gl ہوسٹ کی طرف لے جاتی تھی جو بہت سی ڈیوائسز (devices) میں مال ویئر پھیلا سکتی ہے۔ ماضی میں بھی فیس بک صارفین کو مختلف طریقوں سے بے وقوف بنانے کی کوشش کی گئی۔ مثلاً آپ کو کس کس نے اَن فرینڈ کیا یا کس کس نے آپ کی پروفائل دیکھی جیسے فیچرز حاصل کرنے کے بہانے وائرس زدہ ویب سائٹس پر لے جا کر انھیں نقصان پہنچایا گیا۔

چونکہ صارفین کو ڈِس لائیک بٹن کی اشد ضرورت ہے کیونکہ ہر پوسٹ لائیک کرنے والی نہیں ہوتی اس لیے مارک زکر برگ نے حال ہی اطلاع دی ہے کہ آزمائشی بنیادوں پر لائیک کا نیا بٹن متعارف کروا دیا گیا ہے جس پر کلک کر کے رکھنے سے لائیک کے علاوہ دیگر جذبات کے آئی کنز سامنے آئیں گے۔



اگر کوئی آپ سے پوچھے کہ 2016 میں کون سے شاندار اسمارٹ فون آنے والے ہیں تو آپ شاید کہیں گے سام سنگ گلیکسی ایس 7 یا آئی فون 7۔ کیونکہ یہی فون یا برانڈ ہمارے ہاں زیادہ مقبول ہیں اور انھی کے بارے میں لوگ زیادہ جانتے ہیں یا جاننے کی کوشش کرتے ہیں۔ تاہم کم شہرت یافتہ کمپنیوں کے بھی بہت اچھے اسمارٹ فون عنقریب مارکیٹ میں آنے والے ہیں۔ بہت سے ایسے کم شہرت یافتہ برانڈز ہیں جن کی شہرت سام سنگ یا ایپل سے کم ہے تاہم وہ اچھے فونز بناتے رہتے ہیں جن کے بارے میں موبائل فونز کے شوقین لوگوں کو معلوم ہونا چاہیے۔ ان سے میں سے بعض فونز کی تصاویر تاحال جاری نہیں ہوئیں لیکن یہ کیسے ہو سکتے ہیں یعنی ان کی ممکنہ تصاویر ضرور موجود ہیں۔ اسمارٹ فونز کی دنیا میں سام سنگ اور ایپل کی اجارہ داری کو ختم کرنے کے لیے کئی کمپنیاں سرتوڑ کوشش کر رہی ہیں، اس مضمون کو پڑھ کر آپ اندازہ لگا سکتے ہیں کہ وہ اس میں کامیاب ہوں گی یا نہیں۔

HTC One M10 or HTC 2

یہ ایک قابلِ ذکر فون ہے جو کہ سام سنگ اور ایپل کے لئے خطرہ ثابت ہوسکتا ہے کیونکہ اس کے فیچرز اور ہارڈ ویئر بہت عمدہ ہیں۔ ذرائع کے مطابق اس میں بہترین اسکرین 1920x1080 ریزولیشن کے ساتھ 5.2 انچ ڈسپلے کو سپورٹ کرے گی اور اس کے ڈیزائن میں خوبصورت پتھر ''نیلم'' کا استعمال کیا جائے گا جس سے اس کی مضبوطی میں بہتری آئے گی۔

اس میں 3.1-GHz octa-center 812 پروسیسر موجود ہے جس کی وجہ سے HTC One M10 اگلے سال میں آنے والے کچھ سب سے تیز ترین اسمارٹ فونز میں سے ایک ہوگا۔ اگر HTC کے سابقہ فونز سے اس کا موازنہ کیا جائے تو میگا پکسلز کے لحاظ سے اس کا کیمرا سب سے زبردست ہوگا جس سے حیرت انگیز تصاویر اور ویڈیوز بنائی جاسکیں گی۔

وائرلیس چارجنگ فریم ورک کے ساتھ اس میں moment charging framework بھی شامل ہوگا جس کا فائدہ یہ ہوگا کہ فون بہت جلدی چارج کیا جاسکے گا۔

Apple iPhone 7

اس فون میں نیا A9 کواڈ سینٹر پروسیسر شامل ہوگا جو اسے آج تک کے آنے والے تمام آئی فونز سے تیز بنادے گا۔ 20 میگا پکسلز کا کیمرا اس میں پچھلی سائیڈ پر موجود ہوگا جبکہ سامنے لگے 2 میگا پکسلز کے ایچ ڈی کیمرے کی مدد سے آپ اپنے چاہنے والوں کے ساتھ اعلیٰ معیار کی تصاویر اور سیلفیز بنا سکیں گے۔ اس کی بیٹری کو قدرتی مواد سے بنایا جائے گا جس کی وجہ سے بیٹری زیادہ وقت تک کام کرے گی۔ اس کے علاوہ اس میں ایک حیرت انگیز پروجیکٹر موجود ہوگا جس کی مدد سے آپ کوئی بھی فلم یا پریزنٹیشن (presentation) کسی بھی سطح پر دیکھ سکیں گے۔

LG G5

یہ فون 2016 کے شروع میں آئے گا۔ ذرائع کے مطابق اس میں سب سے نئی اسکرین ٹیکنالوجی اور 5.6 انچ سیفائر اسکرین ہوگی۔ اس کا ڈسپلے اتنا شفاف ہوگا کہ آپ کو لگے گا کوئی اسکرین ہی نہیں لگی ہوئی۔ اس میں 2.9 گیگا ہرٹز آکٹا سینٹر پروسیسر اور پانچ جی بی ریم ہے جس کی وجہ سے آپ کا ہر کام جلدی مکمل ہوجائے گا۔ اس میں قابلِ ذکر پچھلا کیمرا ہے جس کے بارے میں افواہیں ہیں کہ یہ

بیس میگا پکسلز ہوگا اور پانچ میگا پکسلز اگلا کیمرا بھی موجود ہوگا۔

Microsoft Lumia 950 & 950 XL

چونکہ تمام موبائل فونز بنانے والی بڑی کمپنیوں نے اپنے آنے والے فونز کے بارے میں تفصیلات پیش کردی ہیں تو مائیکروسافٹ اس دوڑ میں اینڈرائیڈ فونز کا مقابلہ کرنے میں کیسے پیچھے رہ سکتا ہے۔ توقع یہ کی جارہی ہے کہ مائیکروسافٹ کا آنے والا نیا بہترین اسمارٹ فون Lumia 950 ہو گا جس میں Windows 10 ہوگی۔

کیو ایچ ڈی اسکرین، آکٹا کور اسنیپ ڈریگن پروسیسر، 5.7 انچ ڈسپلے، تین جی بی ریم، دس میگا پکسلز بیک جبکہ پانچ میگا پکسلز فرنٹ کیمرا جیسے فیچرز اسے ایک شاندار اسمارٹ فون بنادیں گے۔

Webs Den Octate

کمپنی کا نام سننے میں آپ کو کچھ عجیب لگ رہا ہوگا لیکن ان کا اوکٹیٹ فون حیران کردینے والی ڈیوائس ہوگا۔ جس میں 1200 x 1920 ریزولوشن کی حامل 5.5 انچ ایل ٹی پی ایس اسکرین موجود ہوگی۔ اس میں 3D کی سپورٹ بھی ہوگی جو اسے 3D فلمیں دیکھنے کے لئے مثالی بنادے گی۔

اس فون میں MediaTek MT6595T پروسیسر ہوگا جس میں آٹھ سینٹرز ہوں گے۔ اس کے علاوہ 3 جی بی ریم جس میں 2GB burst/swap ریم موجود ہوگی جو اس کی کارکردگی کو عمدہ کردیں گے۔ Webs-Den Octate ایک سال بعد تمام موبائل فون کمپنیز کے لئے مشکل حریف ثابت ہو گا اسی لئے ہم نے اس فون کو اس فہرست میں شامل کیا ہے۔

Samsung Galaxy S7

کہا یہ جارہا ہے کہ اسے ستمبر 2016 میں پیش کیا جائے گا۔ اس فون میں ہر وہ خوبی موجود ہوگی جو اسے دنیا کے بہترین فونز کی فہرست میں شامل کردے گی۔

5.1 انچ کی او ایل ای ڈی خمدار اسکرین اس میں زبردست ڈسپلے دے گی۔ 9 گیگا ہرٹز آکٹا سینٹر پروسیسر اور 5 جی بی ریم اس بات کو یقینی بنائیں گے کہ آپ کے تمام گیمز اور اپلی کیشنز بغیر رُکے تیزی سے چلتے رہیں۔

سیلفی کے شوقین افراد کے لیے اس میں زبردست فرنٹ کیمرا دیا جائے گا جس میں 3D کی جدت بھی موجود ہوگی۔ 4000 mAh بیٹری دن بھر استعمال کے بعد بھی ختم نہیں ہوگی۔ مکمل دھاتی باڈی، دھول مٹی اور پانی کے اثرات سے محفوظ رہنے والا یہ فون اس کے علاوہ بھی کئی نئے اور شاندار فیچرز کا مالک ہوگا۔

Nokia C1

نوکیا اپنی گھٹتی ہوئی شہرت کو بچانے کے لئے اگلے سال نئے فونز پیش کرے گا۔ اطلاعات ہیں کہ آنے والے سال میں نوکیا ایک اینڈرائیڈ فون پیش کرے گا جس کا نام C1 ہوگا۔

کہا یہ جارہا ہے کہ اس فون میں 5 انچ آئی پی ایس ڈسپلے، دو جی بی ریم، 8 میگا پکسلز بیک کیمرا جبکہ 5 میگا پکسلز فرنٹ کیمرا موجود ہوگا۔ سب سے مزیدار بات یہ ہے کہ اس میں اینڈرائیڈ لولی پوپ 5.0 ہوگا جس سے لگتا یہ ہے کہ نوکیا اپنی کھوئی ہوئی شہرت کو واپس حاصل کرنے کی بھرپور کوشش کرے گا۔

Oppo Find 9

حالانکہ اوپو ایسا برانڈ نہیں ہے جسے سام سنگ یا ایپل کی طرح شہرت حاصل ہوئی ہو مگر گزشتہ کچھ عرصے میں انہوں نے بہت اچھے فونز پیش کئے ہیں جنہیں فونز کے بہت سے چاہنے والوں نے خراجِ تحسین پیش کیا۔ اوپو کی ایک نئی ڈیوائس Oppo Find 9 اگلے سال پیش کی جائے گی جس میں 1440×2560 ریزولوشن کی حامل 5.5 کیو ایچ ڈی اسکرین ہوگی اپنے زبردست ڈسپلے سے ہر کسی کو چونکا دے گی۔

کہا جارہا ہے کہ اس میں Qualcomm Snapdragon 810 پروسیسر اور چار جی بی ریم ہوگی جس کی وجہ سے آپ اس میں تمام بہترین گیمز کھیل سکیں گے۔ اس میں 20 میگا پکسلز بیک جبکہ 8 میگا پکسلز فرنٹ کیمرا موجود ہوگا جس کی مدد سے آپ عمدہ تصاویر لے سکیں گے۔

Xiaomi Mi 5

یہ فون 2016 کے بہترین فون کے خطاب کے لئے قابلِ ذکر حریف ہے۔ اس میں 5.2 انچ الٹرا ایچ ڈی اسکرین ہے جو اس کے صارف کو بہترین ڈسپلے دِکھائے گی۔ کوالکوم اسنیپ ڈریگن 2.5 گیگا ہرٹز آکٹا سینٹر پروسیسر اس ڈیوائس کی کارکردگی کو بہترین کردے گا۔

اس میں 7 سے لے کر 10 میگا پکسلز تک کے کیمرا ہیں جو کہ یقیناً اس کمپنی کے سابقہ فونز کے کیمروں سے کافی بہتر ہیں۔ اس کے علاوہ اس فون میں وائرلیس چارجنگ، ریٹینا آئی اسکینر وغیرہ جیسے فیچرز موجود ہوں گے جبکہ اس کی بناوٹ میں گلاس میٹل کا استعمال اس فون کی خوب صورتی میں اضافہ کردے گا۔



آئی فون کا بیٹری بیک اَپ بڑھائیں

ایپل اپنے صارفین کے لیے iOS9 جاری کر چکا ہے۔ iOS9 کچھ نئے اور دلچپ فیچرز کے ساتھ پیش کیا گیا ہے تاہم کچھ صارفین سے یہ شکایت موصول ہوئی کہ آئی او ایس کا یہ نیا ورژن پچھلے ورژن کے مقابلے میں بہت زیادہ بیٹری استعمال کرتا ہے۔ اگر آپ کو بھی اس قسم کے مسئلے کا سامنا ہے تو آیئے آپ کو اس کے ممکنہ حل سے آگاہ کرتے ہیں جو آپ کو اَپ گریڈنگ (upgrading) کے بعد آپ کے آئی فون کے بیٹری بیک اپ میں مددگار ثابت ہو گا۔

اپنے فون کو ری اِسٹارٹ کریں

اَپ گریڈنگ کے دوران بہت سارے فیچرز خود ہی چلنا شروع ہو جاتے ہیں اور اَپ گریڈ ہونے کے بعد بھی مسلسل بیک گراونڈ میں چلتے رہتے ہیں لہٰذا اگر آپ کو اَپ گریڈ کرنے کے بعد بیٹری بیک اَپ کا مسئلہ ہو رہا ہے تو آپ کو چاہیے کہ iOS 9 کی انسٹالیشن کے بعد اپنے فون کو ری اِسٹارٹ کریں۔ ری اِسٹارٹ کرنے سے آپ کو یہ بھی معلوم ہو جائے گا کہ آیا کوئی غیر ضروری ایپ (App) بیک گراونڈ میں چل بھی رہی ہے یا نہیں۔ اگر آپ کو ری اِسٹارٹ کرنے کے بعد بھی بیٹری بیک اپ کا مسئلہ ہو رہا ہو تو آپ کے لیے مندرجہ ذیل حل ہیں۔

نئے فیچرز کی جانچ پڑتال نہ کریں

جب بھی ہمیں کوئی نیا فون، اَپ گریڈ، OS یا ایپ ملتی ہے تو ہم اس کی مسلسل جانچ پڑتال (checking) کرتے رہتے ہیں۔ لہٰذا بیٹری بہت جلدی ختم ہونے لگتی ہے۔ اگر آپ نے اپنے آئی فون کو iOS9 پر اَپ گریڈ کیا ہے تو اس کو مسلسل استعمال کرنے کے بجائے کچھ گھنٹوں کے لیے چھوڑ دیں۔ عام طور پر جب ہمارا بیٹری بیک اپ کم ہوتا ہے تو ہمارا خیال اپنے فون کے بارے میں غلط ہونے لگتا ہے جبکہ ہمارا فون استعمال کرنے کا طریقہ غلط ہوتا ہے۔ اس لیے صارفین کے لیے مشورہ ہے کہ اگر آپ اپنے iPhone میں نئے فیچرز، گیمز، ایپس اور کیمرہ وغیرہ استعمال کر رہے ہیں تو اپنے فون کو کچھ دیر کے لیے استعمال کرنا بند کر دیں۔ عام طور پر ہم اپنے بیٹری بیک اپ کو بہتر بنانے کے لیے بہت ساری جانچ پڑتال کرتے رہتے ہیں۔ جبکہ اگر فون صحیح طریقے سے استعمال کریں تو ہماری بیٹری خود ہی اپنا کام اچھے طریقے سے کر رہی ہوتی ہے۔

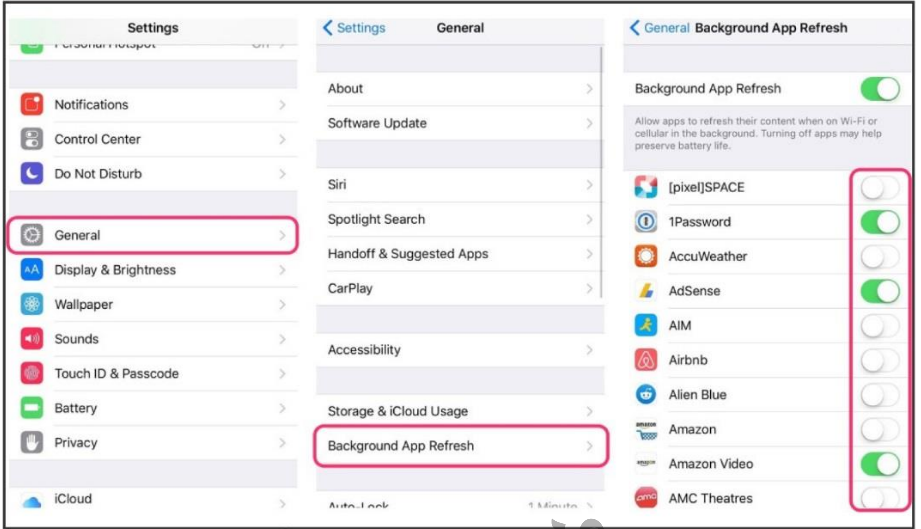
بیٹری کے استعمال کی جانچ پڑتال کریں اور غیر ضروری ایپس کو بند کریں

ios9 بیٹری کے استعمال کے اعداد و شمار (statistics) دِکھا کے آپ کو معلومات فراہم کرتا ہے۔ جس کی مدد سے آپ دیکھ سکتے ہیں کہ آیا بیک گراونڈ پروسیسز زیادہ بیٹری استعمال کر رہے ہیں یا فورگراونڈ ایپس (foreground apps)۔ ان میں سے جو بیٹری زیادہ استعمال کرے، اُسے بند کر دیں تا کہ کچھ بیٹری بیک اپ بچ سکے۔ عام طور پر ای میل اور سوشل نیٹ ورکنگ ایپس جیسے کہ جی میل، فیس بک، ٹوئٹر وغیرہ بہت زیادہ بیٹری استعمال کرتی ہیں۔ لہٰذا آپ ایسی ایپلی کیشنز کو ایک دن کے لیے اَن انسٹال کر کے دیکھیں کہ آیا یہ ایپلی کیشنز بیٹری بیک اپ کم کرنے کی وجہ ہیں یا نہیں۔

مختلف سروِسز کو بند کریں

کچھ دوسرے بیک گراونڈ پروسیسز جیسے کہ لوکیشن سروس (Location Service)، پُش نوٹیفیکیشن (Push Notification) وغیرہ iOS کے بہتر تجربے کو حاصل کرنے کے لیے ضروری ہوتے ہیں۔ یہ چیزیں صارفین کو تازہ ترین صورت حال سے باخبر رکھتی ہیں جیسے نئی ای میل کی فوری اطلاع دینا، فیس بک نوٹیفیکیشن، سکیورٹی نوٹی فکیشن وغیرہ، لیکن یہ بیٹری کو زیادہ خرچ کرتی ہیں۔

غیرضروری استعمال جاری رہتا ہے جو بیٹری بیک اَپ کو کم کردیتا ہے۔ اس صورتِ حال سے نمٹنے کے لیے آئی او ایس 9 میں ایک نیا فیچر ''لو بیٹری موڈ'' شامل کیا گیا ہے۔ اس فیچر کو سیٹنگز میں جاکر بیٹری کے حصے میں فعال کیا جا سکتا ہے۔ اس کے فعال ہونے کی صورت میں خودکار طریقے سے ای میل ایپلی کیشن نئی ای میلز کو چیک نہیں کرتی، بیک گراؤنڈ ایپ ری فریش غیرفعال ہو جاتا ہے، موشن ایفیکٹس اور اینی میٹڈ وال پیپر وغیرہ بھی بند ہو جاتے ہیں۔ اگر آپ کو ای میل دیکھنی ہے تو ای میل ایپلی کیشن کھول کر دیکھنا ہو گا، یہ خود سے نئی میلز کا نہیں بتائے گی۔ ماہرین کا کہنا ہے کہ اس فیچر کے استعمال سے بیٹری بیک اَپ میں تین گھنٹے تک کا اضافہ کیا جاسکتا ہے۔





دوسری چیز ہے بیک گراؤنڈ ایپ ری فریش (Background App Refresh)۔ کچھ ایپلی کیشنز کو بیک گراؤنڈ میں تازہ یعنی ری فریش ہونے کی ضرورت ہوتی ہے تاکہ آپ تازہ ترین اپ ڈیٹس حاصل کرسکیں۔ مثال کے طور پر آپ کی ای میل ایپلی کیشن کو ایک مختصر دورانیے کے بعد خود سے ری فریش ہونے کی ضرورت ہوتی ہے تاکہ آپ کی تازہ ترین ای میلز ظاہر ہو جائیں۔ دوسری طرف فیس بُک کو بھی خود سے ری فریش ہونے کی ضرورت ہوتی ہے، تاکہ آپ کو تازہ ترین نوٹی فکیشنز میں بتا سکے کہ فیس بک پر کسی نے آپ کو کوئی پیغام، کوئی دوست بننے کی درخواست تو نہیں بھیجی یا پھر کسی نے آپ کی پوسٹ کو لائیک کیا ہے یا پھر اپنی کسی تصویر میں آپ کو ٹیگ کیا ہے وغیرہ۔

ایل ٹی ای زیادہ بیٹری استعمال کرتا ہے

عام طور پر 2G کے مقابلے میں 3G زیادہ بیٹری استعمال کرتا ہے۔ بالکل اسی طرح 3G کے مقابلے میں 4G LTE زیادہ بیٹری استعمال کرتا ہے۔ ایپل کے مطابق آئی فون 6S ایل ٹی ای (LTE) پر بارہ گھنٹے تک انٹرنیٹ استعمال کرنے کے قابل ہے لیکن یہ وقت دن بدن کم ہوتا رہتا ہے۔ آپ یہ توقع نہیں کرسکتے کہ ایل ٹی ای پر آٹھ گھنٹے سے زیادہ انٹرنیٹ استعمال کیا جاسکتا ہے۔

لو بیٹری موڈ (Low Power Mode)

زیادہ تر لوگ فون کے آپریٹنگ سسٹم کی سیٹنگز میں زیادہ تبدیلیاں نہیں کرتے، نہ ہی ایپلی کیشنز کی نوٹی فکیشنز کو بند کرتے ہیں بلکہ جو چیز جیسی مل جائے ویسے ہی استعمال کرتے رہتے ہیں، یہی وجہ ہے کہ فون بیٹری کا بے دریغ

اختتامیہ

اگر مندرجہ بالا بتائے گئے حل میں سے کوئی بھی کام نہ کرے تو اپنا آئی فون کسی ماہر کے پاس لے جائیں تاکہ معلوم ہو سکے کہ آیا بیٹری میں کوئی مسئلہ ہے یا نہیں۔ عام طور پر یہ ایک بہت ہی غیر معمولی مسئلہ ہے۔ مگر اس بات کی کوئی ضمانت نہیں کہ ایک بیٹری بغیر کسی مسئلے کے چار سال چلے۔

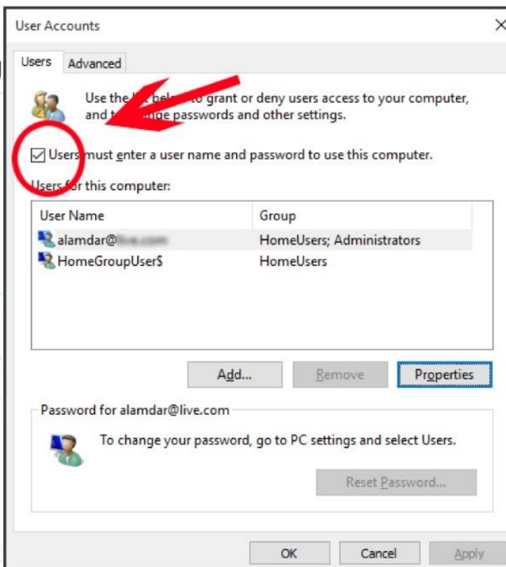


ونڈوز 10 کو کچھ تیز رفتار بنائیں

کیا آپ ونڈوز 10 استعمال کر رہے ہیں اور اسے تیز رفتار بنانا چاہتے ہیں؟ تو آیئے آپ کو تین آسان ٹپس بتاتے ہیں جنھیں استعمال کرتے ہوئے آپ ونڈوز 10 آپریٹنگ سسٹم کو برق رفتار بنا سکتے ہیں۔

تیز اسٹارٹ اپ

جب بھی آپ سسٹم آن کرتے ہیں ونڈوز کے لوڈ ہوتے ہی پاس ورڈ ٹائپ کرنا پڑتا ہے۔کیا آپ اس پاس ورڈ کی جھنجھٹ سے آزاد ہونا چاہتے ہیں کہ پی سی آن ہوتے ہی خود بخود ڈیسک ٹاپ سامنے آجائے؟ تو اس کے لیے RUN میں netplwiz لکھ کر اینٹر پریس کردیں۔''یوزر اکاؤنٹس'' کی ایپلٹ کھل جائے گی۔ یہاں "...Users must enter" کے ساتھ موجود چیک باکس کو اَن چیک کرتے ہوئے OK کے بٹن پر کلک کر دیں۔ لیجیے اب ونڈوز کے لوڈ ہونے پر پاس ورڈ ٹائپ نہیں کرنا پڑے گا بلکہ پی سی آن ہوتے ہی ڈیسک ٹاپ سامنے آجائے گا۔



تیز اسٹارٹ مینو

اگر آپ کے پاس اسٹارٹ مینو لوڈ ہونے میں دیر لگتا ہے تو اس کا مطلب ہے آپ کا پی سی اینی میشن لوڈ کرنے کے قابل نہیں جسے انتہائی زیادہ پی سی ریسورسز درکار رہوتی ہیں۔اسٹارٹ مینو کو تیز بنانے کے لیے اینی میشن کو غیر فعال کیا جاسکتا ہے۔اس کے لیے RUN میں sysdm.cpl لکھ کر اینٹر پریس کریں۔ سسٹم پراپرٹیز کھل جائیں گی۔

یہاں Advanced کے ٹیب میں آکر پرفارمنس کے ذیل میں موجود Settings کے بٹن پر کلک کریں۔

اگلی کھلنے والی ونڈو میں Animate windows when minimizing and maximizing کے ساتھ موجود باکس کو اَن چیک کردیں۔

تیز شٹ ڈاؤن

ونڈوز 10 کو شٹ ڈاؤن کرنے کے لیے تین دفعہ کلک کرنا پڑتا ہے۔اگر آپ صرف ایک کلک سے یہ کام کرنا چاہتے ہیں تو ڈیسک ٹاپ کی کسی خالی پر رائٹ کلک کرتے ہوئے نیا شارٹ کٹ بنالیں۔شارٹ کٹ لوکیشن مانگے گا اس میں درج ذیل کمانڈ ٹائپ کریں:

```
%windir%\System32\shutdown.exe /s /t 0
```

اس کمانڈ سے ونڈوز کو شٹ ڈاؤن کرنے کے لیے ڈیسک ٹاپ پر شارٹ کٹ بن جائے گا۔جب بھی پی سی شٹ ڈاؤن کرنا ہو اس پر کلک کردیں۔

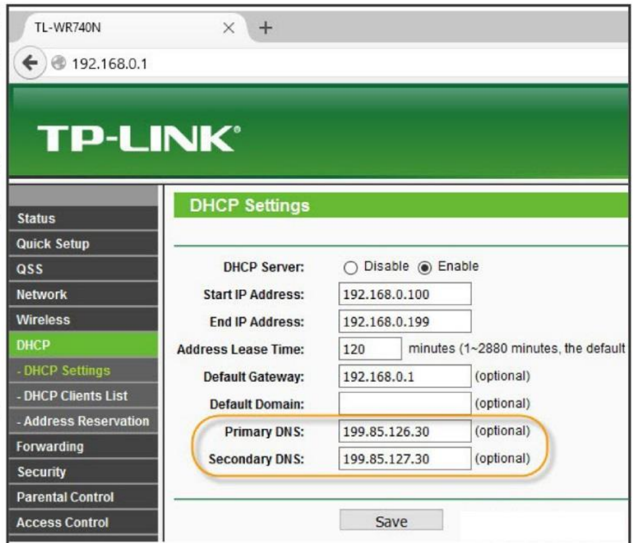
انٹرنیٹ کو بچوں کے لیے محفوظ بنائیں

آج کل کمپیوٹر ہر گھر میں موجود ہے اور بچوں کا کمپیوٹر استعمال کرنا لازمی ہو چکا ہے بلکہ کمپیوٹر استعمال کرنے والے بچوں کو ذہین تصور کیا جاتا ہے۔ کمپیوٹر موجود ہو اور انٹرنیٹ نہ ہو؟ یہ تو ممکن نہیں۔ بچوں کو ذاتی کمپیوٹر فراہم کرنے والے والدین اکثر پریشان رہتے ہیں کہ کہیں ان کے بچے انٹرنیٹ کی برائیوں کا نشانہ نا بن جائیں۔ پیرینٹل کنٹرول کے ویسے تو کئی سافٹ ویئر اور ایپلی کیشنز دستیاب ہیں لیکن یہ کام وائی فائی راؤٹر کی کنفگریشن بدل کر بھی کیا جا سکتا ہے۔

انٹرنیٹ کو بچوں کے لیے محفوظ بنانے کے لیے وائی فائی راؤٹر کی DNS سیٹنگز کو بدلنا ہوگا۔ یہ کام آپ با آسانی صرف دو منٹس میں مکمل کر سکتے ہیں۔ اس کے آغاز کے لیے اپنے راؤٹر کا ویب انٹرفیس کھول لیں۔ عموماً اس انٹرفیس کو دیکھنے کے لیے براؤزر میں 192.168.0.1 یا پھر 192.168.1.1 ٹائپ کرنا ہوتا ہے۔ یہاں آپ سے لاگ اِن ہونے کا کہا جائے گا۔ عام طور پر راؤٹر کا یوزر نیم admin اور پاس ورڈ بھی admin ہوتا ہے۔ اگر آپ راؤٹر کا ویب انٹرفیس نہیں دیکھ پا رہے تو راؤٹر کے ڈبے یا ڈبے میں موجود ڈاکیومنٹ دیکھیں، اس پر یہ تفصیل ضرور موجود ہوتی ہے۔

راؤٹر کے ویب انٹرفیس میں آپ کو DHCP سیٹنگز میں جانا ہوگا۔ یہاں DNS کی تفصیلات موجود ہوں گی۔ آپ یہاں کوئی بھی مفت دستیاب ڈی این ایس ڈال سکتے ہیں جو خطرناک ویب سائٹس کو بلاک کرتا ہو، ایسے تین ڈی این ایس سرور دستیاب ہیں:

☆ نورٹن کنیکٹ سیف (Norton ConnectSafe)



https://dns.norton.com

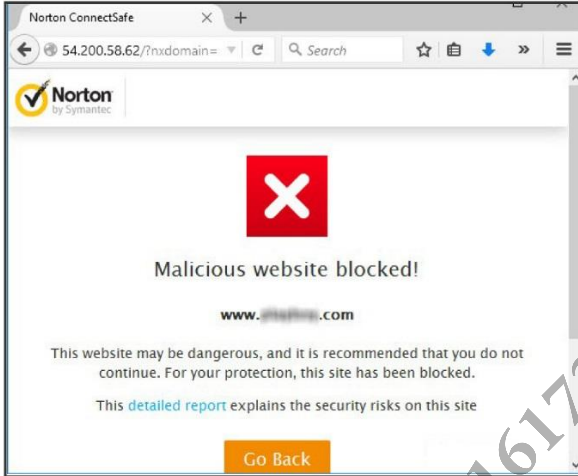
☆ اوپن ڈی این ایس فیملی (OpenDNS Family)

http://www.opendns.com

☆ وائے انڈیکس فیملی (Yandex Family)

http://dns.yandex.com

نورٹن کنیکٹ سیف کی بات کی جائے تو اس کا پرائمری سرور 199.85.126.30 جبکہ سیکنڈری سرور 199.85.127.30 ہے۔



اپنے راؤٹر کے ڈی این ایس میں آپ یہ ایڈریس ٹائپ کر سکتے ہیں۔ سیٹنگز کو محفوظ کرنے کے بعد راؤٹر کو ایک دفعہ ری اسٹارٹ کر لیں۔ اس کے بعد آپ کے انٹرنیٹ پر کھلنے سے پہلے تمام ویب سائٹس کا جائزہ نورٹن لے گا اور اگر وہ نقصان دہ یا بچوں کے لیے ناموزوں ہوں گی تو انھیں بلاک کر دیا جائے گا۔

''اوپن ڈی این ایس فیملی'' بھی ایک اچھی سروس ہے جسے خاص طور پر خاندان اور اسکولوں کے لیے بنایا گیا ہے۔ آپ اس ڈی این ایس کو بھی استعمال کر سکتے ہیں:

Primary DNS: 208.67.222.123

Secondary DNS: 208.67.220.123

Yandex Family ڈی این ایس سرورز روسی سرچ انجن کمپنی ''وائے انڈیکس'' کے ہیں۔ آپ چاہیں تو اسے بھی استعمال کر سکتے ہیں:

Primary DNS: 77.88.8.7

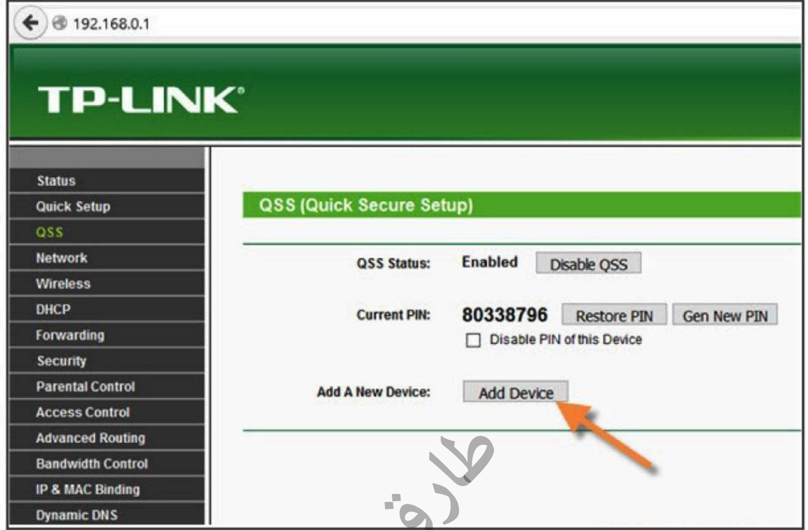
Secondary DNS: 77.88.8.3

اپنے وائی فائی راؤٹر سے بذریعہ WPS کنیکٹ ہوں

وائی فائی کی حامل ڈیوائسز کو کئی طریقوں سے وائی فائی راؤٹر سے کنیکٹ کیا جا سکتا ہے۔ سب سے عام رائج طریقہ یہی ہے کہ ڈیوائس پر وائی فائی نیٹ ورک تلاش کرتے ہوئے اپنے منتخب کردہ نیٹ ورک یا ہاٹ اسپاٹ سے بذریعہ پاس ورڈ (WPA/WPA2) کنیکٹ ہوا جاتا ہے۔ یہ وہی طریقہ جس سے آپ تقریباً روزانہ اپنے وائی فائی نیٹ ورک کو کنیکٹ کرتے ہیں۔

کیا آپ کو معلوم ہے کہ وائی فائی راؤٹر سے کسی اور طرح بھی کنیکٹ ہوا جا سکتا ہے؟ جی ہاں ایک بہت ہی سادہ اور محفوظ طریقہ بھی موجود ہے جس میں بذریعہ WPS یعنی وائی فائی پروٹیکٹڈ سیٹ اپ کنیکٹ ہوا جاتا ہے۔ عموماً اسے WPS ہی کہا جاتا ہے لیکن کچھ راؤٹرز میں اس کا مختلف نام بھی ہوسکتا ہے مگر طریقہ کار ایک ہی ہے۔ مثال کے طور پر TP-LINK کے راؤٹرز میں اسے QSS کہتے ہیں یعنی کوئیک سیکیور سیٹ اپ۔

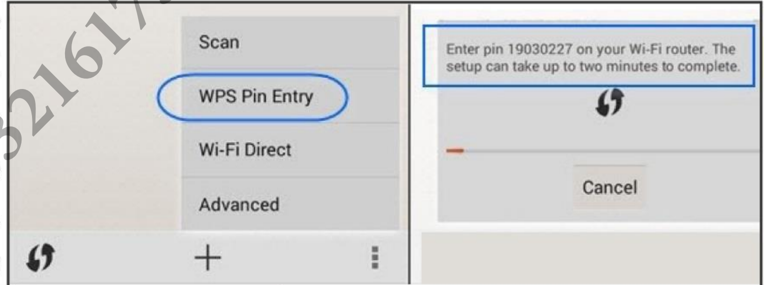
آیئے آپ کو بتاتے ہیں کہ کس طرح ڈبلیو پی ایس کو استعمال کرتے ہوئے وائی فائی راؤٹر سے جڑا جاتا ہے۔



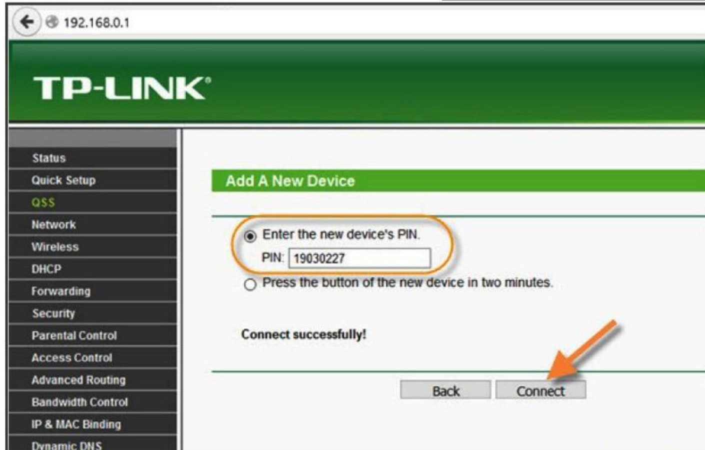
سب سے پہلے اپنے راؤٹر کا ویب انٹرفیس کھول لیں۔ عموماً اس انٹرفیس کو دیکھنے کے لیے براؤزر میں 192.168.0.1 یا پھر 192.168.1.1 ٹائپ کرنا ہوتا ہے۔ یہاں آپ سے لاگ اِن ہونے کا کہا جائے گا۔ عام طور پر راؤٹر کا یوزر نیم admin اور پاس ورڈ بھی admin ہوتا ہے۔ اگر آپ راؤٹر کا ویب انٹرفیس نہیں دیکھ پا رہے تو راؤٹر کے ڈبے یا ڈبے میں موجود ڈاکیومنٹ دیکھیں، اس پر یہ تفصیل ضرور موجود ہوتی ہے۔

ڈبلیو پی ایس یا کیو ایس ایس میں آنے کے بعد Add Device کے بٹن پر کلک کریں۔

اب اپنے اینڈرویڈ فون کی وائی فائی سیٹنگز میں آکر مینو میں سے WPS Pin Entry کو منتخب کریں۔ یہ آپ کو ایک PIN بتائے گا۔ اس پن کو نوٹ کر لیں کیونکہ اسے وائی فائی راؤٹر میں درج کرنا ہوگا۔



دوبارہ راؤٹر کے ویب انٹرفیس میں آئیں اور ''ایڈ ڈیوائس'' کے بعد آپ کو پن درج کرنے کا کہا جا رہا ہوگا۔ وہاں پن درج کرنے کے بعد Connect کے بٹن پر کلک کر دیں۔ چند لمحوں میں آپ کا اینڈرویڈ فون آپ کے راؤٹر سے کنیکٹ ہوجائے گا۔ اب آپ بذریعہ WPS انٹرنیٹ استعمال کر سکتے ہیں۔

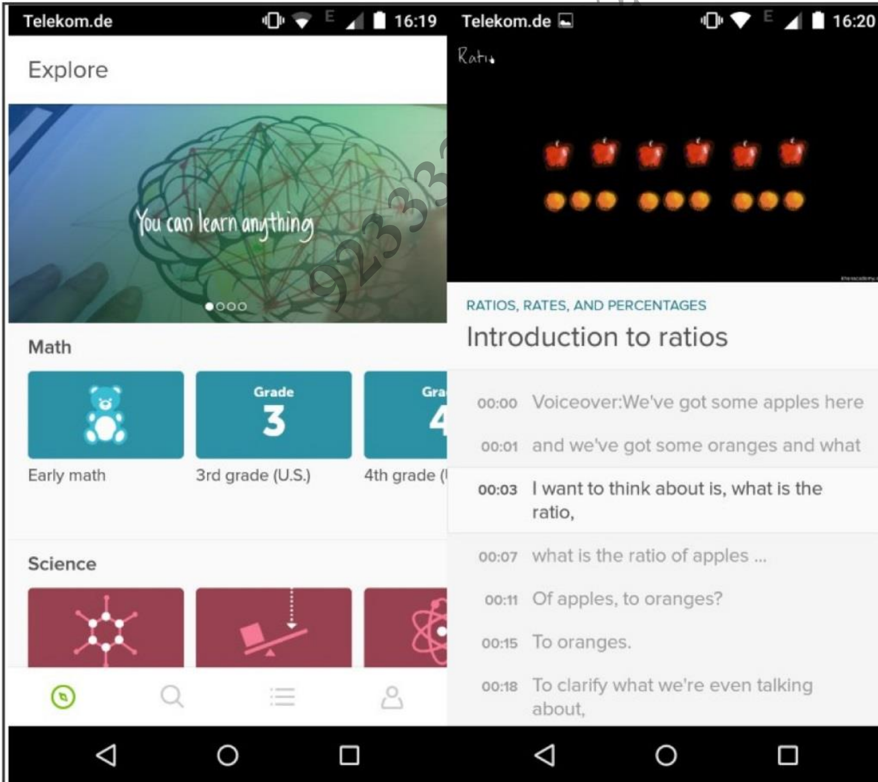


خان اکیڈمی کی اینڈرائیڈ ایپلی کیشن ریلیز

"خان اکیڈمی" آن لائن تعلیم کا ایک بہترین ذریعہ ہے۔ خان اکیڈمی کی ویب سائٹ پر تقریباً تمام مضامین کے بارے میں اسباق موجود ہیں۔ اس کی خاص بات ہر چیز کا بہت ہی واضح انداز اور باتصویر ہونا ہے جو طالب علموں کو سمجھنے میں آسانی پیدا کرتا ہے۔

سائنس ہو، ریاضی ہو یا کمپیوٹر کا علم خان اکیڈمی پر تقریباً ہر موضوع پر اسباق آپ کو ملیں گے۔ خان اکیڈمی کی وجہ شہرت ہر بات کو وڈیو کے ذریعے سمجھانا ہے۔ اس کے علاوہ وڈیو میں سمجھانے کا بہت ہی آسان طریقہ اور سادہ زبان استعمال کی جاتی ہے۔ اگر آپ ریاضی کے حوالے سے کسی مسئلے کا شکار ہیں تو خان اکیڈمی کی ویب سائٹ پر جائیں، وہاں اس حوالے سے مددگار وڈیو دیکھیں اور اس سوال کو حل کرنا سیکھیں۔

خان اکیڈمی کسی تعریف کی محتاج نہیں، ان کا ذکر ہم پہلے بھی کئی بار کمپیوٹنگ میں کر چکے ہیں اور امید ہے آپ بھی ان سے واقف ہوں گے۔ خان اکیڈمی کو پہلی بڑی کامیابی گوگل کی جانب سے دیا گیا انعام ہے اور خان اکیڈمی نے انعام میں ملی رقم کو اپنے پروجیکٹ پر خرچ کرتے ہوئے اپنے معیار کو مزید بہتر بنایا۔



شاید اسی سلسلے کی ایک کڑی اب خان اکیڈمی اینڈرائیڈ ایپ ہے۔ جی ہاں ان کی اینڈرائیڈ ایپ ریلیز ہو چکی ہے، یعنی اب آپ تعلیم کا سلسلہ جہاں چاہیں اپنی فون کے ذریعے شروع کر سکتے ہیں۔

بالکل ویب سائٹ کی طرح ایپلی کیشن میں تمام موضوعات، کلاسیں اور لیکچرز وغیرہ موجود ہیں۔ پہلے ہی صفحے پر موضوعات اور گریڈ کے اعتبار سے کلاسوں کو ترتیب دیا گیا ہے۔ جیسے کہ اگر آپ کو بائیولوجی اور فزکس کے حوالے سے پڑھنا ہو تو سائنس کے حصے میں آجائیں۔

کسی بھی کلاس کے بارے میں مزید تفصیلات جاننے کے لیے اس پر ٹچ کریں تو اس میں موجود تمام دستیاب اسباق سامنے آجائیں گے۔ کسی خاص موضوع پر جانے کے لیے بھی براہِ راست اس پر ٹچ کیا جا سکتا ہے۔

جب آپ کسی موضوع کو منتخب کرلیں گے تو اس حوالے سے یوٹیوب وڈیو اوپر موجود ہوگی جبکہ اس کے بارے میں مواد نیچے دکھایا جائے گا۔

اگر آپ پہلے سے خان اکیڈمی کی ویب سائٹ پر اکاؤنٹ رکھتے ہیں تو اسی اکاؤنٹ کو ایپلی کیشن میں بھی استعمال کر سکتے ہیں اس طرح آپ نے ویب سائٹ پر جو پیش رفت کی ہوگی وہ ایپلی کیشن میں بھی ظاہر ہو جائے گی۔

ایپلی کیشن میں کئی اچھے فیچرز شامل کیے گئے ہیں جیسے کہ آپ اس میں اپنی وڈیوز بھی شامل کر سکتے ہیں، اس کے علاوہ اگر آپ کوئی وڈیو دیکھتے ہوئے ایپلی کیشن بند کر دیں گے تو اگلی دفعہ ایپلی کیشن کھولنے پر وہ وڈیو آپ کو چھوڑی گئی جگہ سے ہی دکھائی جائے گی تاکہ آپ وہیں سے سلسلہ دوبارہ شروع کر سکیں۔

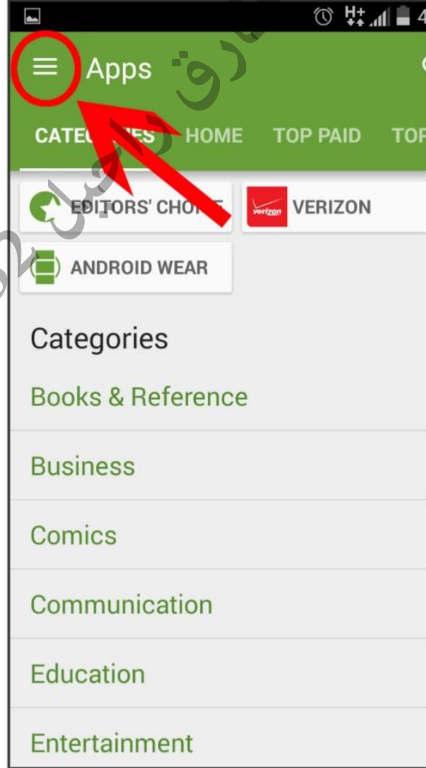
خان اکیڈمی کی اینڈرائیڈ ایپلی کیشن یقیناً ان کے لاکھوں طالب علموں کے لیے انتہائی مفید ثابت ہوگی۔

bit.ly/khanacademy-android

اینڈرویڈ پر ایپلی کیشنز کی اپ ڈیٹس کی نوٹی فکیشنز بند کریں

اینڈرویڈ ایپلی کیشنز بہت تیزی سے اپ ڈیٹس ہوتی ہیں۔ ایپلی کیشنز کی اپ ڈیٹس کو ہمیشہ خوش آمدید کہنا چاہیے کیونکہ یہ اپنے ساتھ نئے فیچرز اور پرانے مسائل کے حل لاتی ہیں۔ لیکن کبھی کبھار ایپلی کیشنز کی اپ ڈیٹس کی اطلاع بہت کوفت کا شکار کرتی ہے۔ اینڈرویڈ میں یہ پہلے سے سیٹنگز ہوتی ہیں کہ انسٹال کسی بھی ایپلی کیشن کی اپ ڈیٹس جاری ہوں تو اطلاع کرے، بلکہ وائی فائی پر موجود ہونے کی صورت میں اپ ڈیٹس خود بخود ڈاؤن لوڈ ہو کر انسٹال بھی ہو جاتی ہیں تب آپ کو خبر ہوتی ہے۔

اگر آپ چاہیں کہ اپ ڈیٹس کی نوٹی فکیشنز بند ہو جائیں بلکہ آپ جب چاہیں کچھ دن بعد خود اپ ڈیٹس دیکھیں اور انسٹال کریں تو اینڈرویڈ میں یہ بھی ممکن ہے۔



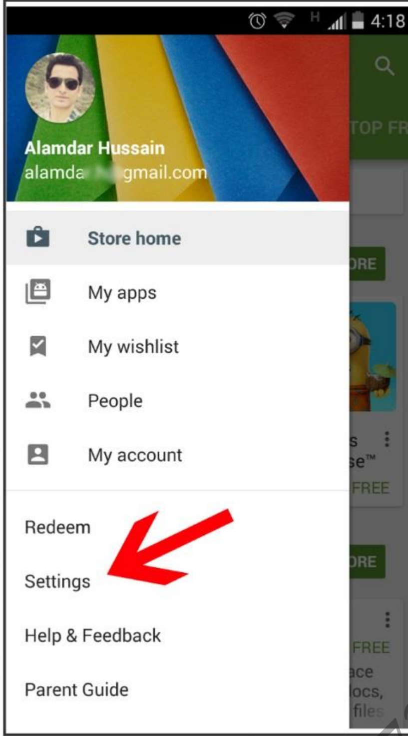
اس کام کے لیے سب سے پہلے گوگل پلے اسٹور کھول لیں۔

اسٹور کھل جائے تو اس میں سب سے اوپر بائیں طرف موجود تین لائنوں والے مینو پر ٹچ کریں۔

مینو کھل جائے تو اس میں سیٹنگز پر ٹچ کرتے ہوئے سیٹنگز میں آجائیں۔

سیٹنگز میں آپ دیکھ سکتے ہیں کئی اہم آپشنز موجود ہیں۔ جیسے کہ ایپلی کیشنز کس انٹرنیٹ پر اپ ڈیٹ ہوں جیسے کہ وائی فائی پر ایپلی کیشنز کا اپ ڈیٹ ہونا پہلے سے سیٹ ہوتا ہے۔ اس کے علاوہ یہاں یہ آپشن بھی موجود ہے کہ ہر نئی انسٹال ہونے والی ایپلی کیشن کا آئی کن ہوم اسکرین پر ڈالا جائے۔

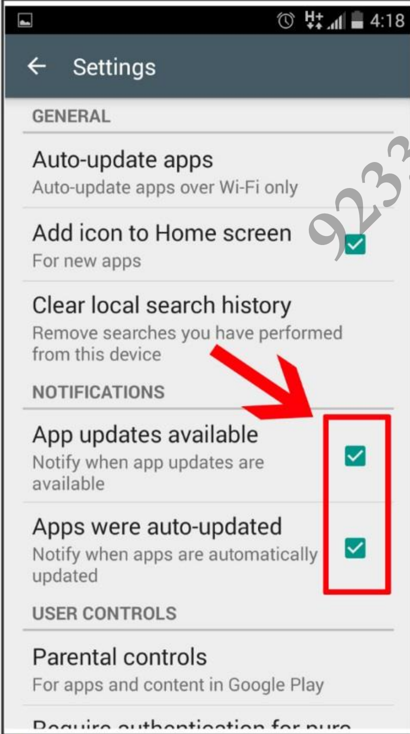
لیکن چونکہ ہمارا مقصد ایپلی کیشنز کی اپ ڈیٹس کی نوٹی فکیشنز کو بند کرنا ہے تو یہاں اس حوالے سے دو آپشنز موجود ہیں۔



پہلا آپشن ہے کہ ایپلی کیشن کی اپ ڈیٹس کی دستیابی کا نوٹی فکیشن دیا جائے۔

جبکہ دوسرا آپشن ہے کہ ایپلی کیشن جب خودکار طریقے سے اپ ڈیٹ ہو جائے تو مطلع کر دیا جائے۔

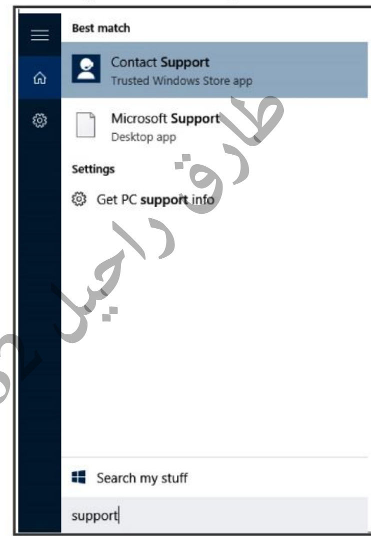
چونکہ ہمارا مقصد ان دونوں نوٹی فکیشنز سے جان چھڑانا ہے اس لیے دونوں کے ساتھ موجود چیک باکسز کو ان چیک کر دیں۔



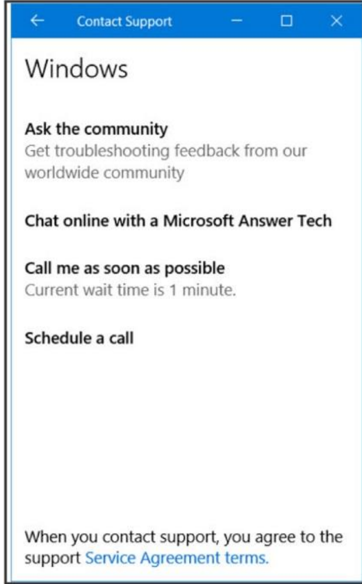
لیجیے یہ کام مکمل ہو چکا ہے۔ لیکن اب یاد رہے کہ آپ کی انسٹال ایپلی کیشنز اس وقت تک اپ ڈیٹ نہیں ہوں گی جب تک آپ دوبارہ پلے اسٹور میں آ کر ان کی اپ ڈیٹس چیک کریں گے۔

ونڈوز 10 میں کوئی خرابی براہِ راست مائیکروسافٹ کے انجینئر سے ٹھیک کروائیں

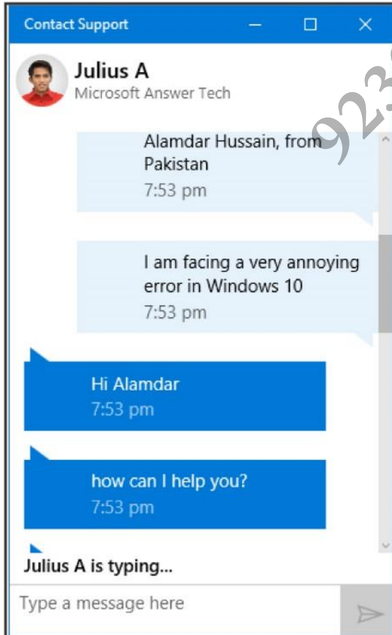
ونڈوز 10 کے کئی اہم اور نئے فیچرز میں سے ایک فیچر سپورٹ کا بھی ہے۔ اس دفعہ مائیکروسافٹ نے اپنے صارفین کی خدمت کرنے میں کوئی کسر نہیں چھوڑی۔ آپ کو انٹرنیٹ ایکسپلورر، ایج، ون ڈرائیو، آفس، ایکس باکس، بنگ میں کوئی مسئلہ آرہا ہے، ونڈوز ایکٹی ویٹ نہیں ہو پارہی ہے یا کوئی بھی ایرر آپ کو تنگ کررہا ہے تو براہِ راست مائیکروسافٹ سے مدد کے لیے رابطہ کیا جاسکتا ہے۔ رابطے کے لیے پرانے ٹکٹ سسٹم کی بجائے آپ کو فوراً مدد فراہم کی جائے گی چاہے اس کے لیے مائیکروسافٹ انجینئر کو فون کرنا پڑے یا چیٹ کرنی پڑے۔



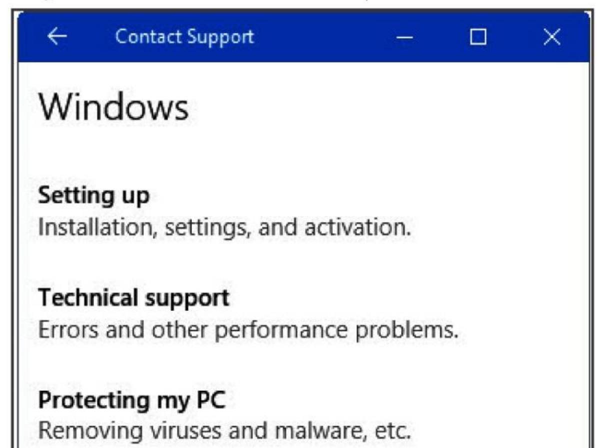
سب سے سہل طریقہ یہ ہے کہ آپ چیٹ کا انتخاب کریں۔ چیٹ شروع کرنے سے پہلے آپ کو اپنا فون نمبر بھی دینا ہوگا تاکہ اگر آپ کا رابطہ منقطع ہوجائے تو انجینئر آپ کو فون کر سکے۔ اگر آپ چیٹ کا انتخاب کریں گے اور آپ کا مسئلہ ایسا ہے کہ اسے ٹھیک کرنے کے لیے انجینئر کو آپ کے ڈیسک ٹاپ تک رسائی حاصل کرنی ہو تو وہ اس کی بھی اجازت چاہیں گے۔ اس طرح انجینئر آپ کے سسٹم تک بذریعہ ریموٹ ڈیسک ٹاپ رسائی کے لیے ایک ٹول فراہم کرے گا، وہ ٹول انسٹال کرنے کے بعد آپ کی اجازت سے آپ کا ڈیسک ٹاپ انجینئر کے لیے قابلِ رسائی ہو گا۔ رابطہ جُڑنے کے بعد ماؤس چھوڑ دیں اور باقی کام انجینئر صاحب پر چھوڑ دیں، وہ آپ کا مسئلہ حل کردیں گے۔



یعنی اب کمپیوٹر کے مسائل ٹھیک کرانے کے لیے دوستوں کے نخرے اُٹھانے کی ضرورت نہیں بلکہ براہِ راست مائیکروسافٹ کو زحمت دیں۔ اس کے لیے اسٹارٹ کے بٹن پر کلک کرتے ہوئے Support ٹائپ کریں اور سامنے آنے والے Contact Support پر کلک کردیں۔ سپورٹ ایپلی کیشن کھل جائے گی اور مائیکروسافٹ کی مددگار لائن سے رابطہ کرنے کی کوشش شروع کردے گی۔ رابطہ ہوجانے کے بعد آپ کو درپیش مسئلے کی کیٹیگری منتخب کرنی ہوگی۔



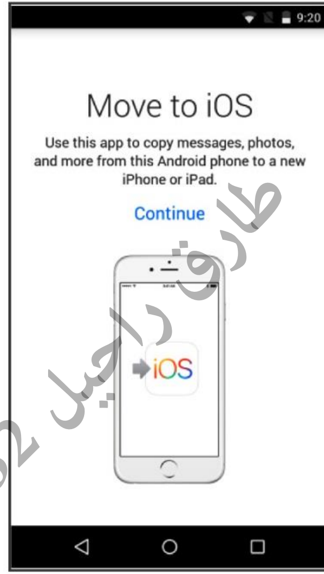
درست کیٹیگری کے انتخاب کے بعد پوچھا جائے گا کہ آپ کس طرح مدد حاصل کرنا چاہتے ہیں مثلاً چیٹ کرنا چاہتے ہیں یا کال شیڈول کرنا چاہتے ہیں۔ اپنی پسند کے تحت آپشن منتخب کرلیں۔ اس طرح آپ باآسانی مائیکروسافٹ سے رابطہ کرکے ونڈوز کے مسائل ٹھیک کرسکتے ہیں۔



اپیل کی ایپ کی مدد سے اینڈ رویئڈ فون سے آئی او ایس پر با آسانی منتقل ہوں

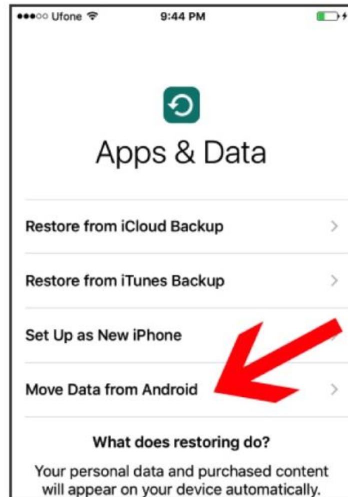
کچھ عرصہ پہلے گوگل نے یہ آسانی فراہم کی کہ جو لوگ آئی فون استعمال کر کے اُکتا چکے ہیں وہ اپنے فونز کو اینڈ رویئڈ پر منتقل کر سکتے ہیں۔ اس کے لئے با قائدہ اینڈ رویئڈ کی ویب سائٹ پر ایک صفحہ بنایا گیا ہے جو آپ کے ڈیٹا کو آئی او ایس سے اینڈ رویئڈ ڈیوائس پر منتقلی میں مدد کرتا ہے۔

www.android.com/switch



9 ستمبر 2015 کو اپیل نے جوابی وار کیا اور ایک نئی ایپ متعارف کروائی موو ٹو آئی او ایس (Move to iOS)۔ اپیل کی یہ پہلی اور شاید آخری اینڈ رویئڈ ایپ ہوگی جس کے نام سے صاف ظا ہر ہے کہ یہ ایپ آپ کو اینڈ رویئڈ ڈیوائس سے آئی فون پر منتقل ہونے میں مدد کرتی ہے۔ آپ سوچ رہے ہوں گے کہ یہ کیسے ممکن ہے اور کس طرح کیا جا سکتا ہے لہٰذا مندرجہ ذیل بتائے گئے طریقے کار کو ملاحظہ کریں۔

اینڈ رویئڈ فون پر کیا کرنا چاہیے



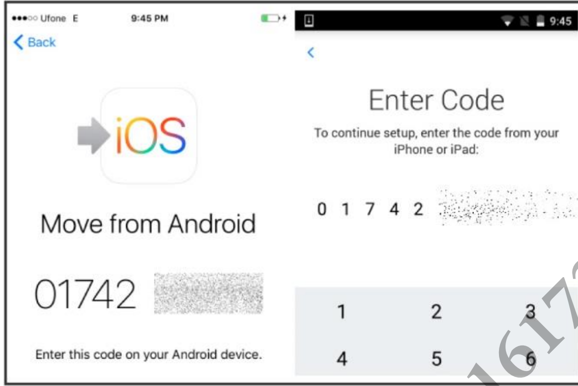
موو ٹو آئی او ایس کو گوگل کے پلے اسٹور سے انسٹال کریں پھر اُسے کھولیں۔

bit.ly/moveto-ios

اس بات کی یقین دہانی کر لیجیے کہ آپ کی ڈیوائس مکمل چارج ہے یا پھر چارجنگ پر لگی ہوئی ہے۔ اس کے علاوہ انٹرنیٹ کا چل رہا ہونا بھی ضروری ہے۔

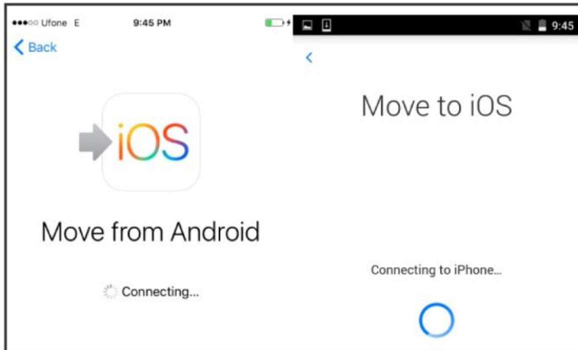
آئی فون پر کیا کرنا چاہیے

ہم یہ مان لیتے ہیں کہ آپ نے نیا فون لیا ہے۔ اپنی آئی فون ڈیوائس کو کھولیں پھر اسے اپنے نام پر رجسٹر کروائیں۔ وائی فائی سے کنیکٹ کریں۔ اپیل کی ID بنانے کو نظرانداز کیا جا سکتا ہے کیونکہ ڈیٹا منتقل کرتے وقت اس کی ضرورت پیش نہیں آتی۔ اس کے بعد سیٹ اپ آپشنز (Set-up options) میں جا کر یہ فیصلہ کیا جا سکتا ہے کہ آپ اپنی ڈیوائس کو نئے فون کے طور پر استعمال کرنا چاہتے ہیں، بیک اپ ڈیٹا کو بحال کرنا چاہتے ہیں یا اینڈ رویئڈ سے ڈیٹا منتقل کرنا چاہتے ہیں۔ آخری آپشن کو منتخب کریں اور اگلے پیج کی جانب بڑھ جائیں۔



اینڈ رویئڈ اور آئی فون پر مشترکہ کیا کرنا چاہیے

اسکرین شاٹ کی طرح بائیں جانب میں آئی فون میں دیئے گئے کوڈ کو دیکھا جا سکتا ہے اور دائیں جانب اسکرین شاٹ میں یہ بتایا گیا ہے کہ اینڈ رویئڈ ڈیوائس میں موو ٹو آئی او ایس ایپ میں کہاں اُس کوڈ کا اندراج کرنا ہے۔ دونوں فونز میں رابطہ جُڑتے ہی ڈیٹا منتقلی کا کام شروع ہو جائے گا۔



ونڈوز 10 میں ''ونڈوز ڈیفینڈر'' کو غیر فعال (Disable) کریں

ونڈوز 10 میں حفاظتی پروگرام ''ونڈوز ڈیفینڈر'' پہلے سے موجود ہوتا ہے تا کہ آپ کو اینٹی وائرس انسٹال کرنے کی ضرورت نہ پڑے۔ اگر آپ اسے باقاعدگی سے اپ ڈیٹ کرتے رہیں تو یہ آپ کو خطرناک پروگرامز اور مال ویئر وغیرہ سے بچا سکتا ہے۔ لیکن جب اس سے اچھے اینٹی وائرس موجود ہیں تو کیوں نا انھیں استعمال کریں؟ ویسے زیادہ لوگوں کو ونڈوز ڈیفینڈر پسند بھی نہیں ہوتا، کسی کو اے وی جی اینٹی وائرس پسند ہے تو کسی کو اواسٹ۔ ونڈوز ڈیفینڈر کو دیکھا جائے تو یہ ایک سادہ سا اینٹی وائرس ہے، جبکہ اس کے مقابلے میں درجنوں جدید اینٹی وائرس دستیاب ہیں تو کیوں نا ونڈوز ڈیفینڈر کو غیر فعال یعنی ڈس ایبل کر دیا جائے تاکہ کوئی دوسرا اینٹی وائرس استعمال کیا جا سکے؟

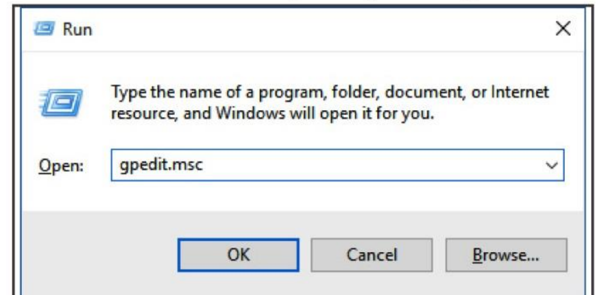
ونڈوز ڈیفینڈر کو غیر فعال کرنے سے پہلے بہتر ہے کہ کوئی اینٹی وائرس انسٹال کر لیں تا کہ آپ کا سسٹم کسی بھی لمحے غیر محفوظ نہ رہے۔ اگر آپ اینٹی وائرس کے انتخاب میں پریشان ہیں تو وائرس ٹوٹل کی ویب سائٹ کے اس صفحے پر اینٹی وائرس پروگرامز کی فہرست دیکھیں:

virustotal.com/en/about/credits

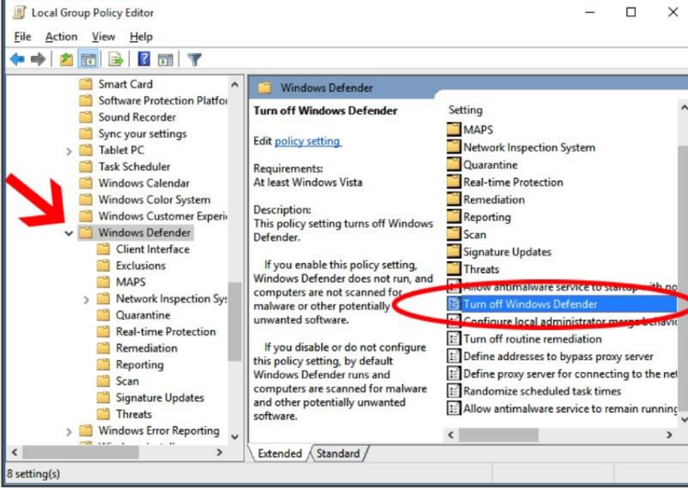
کمپیوٹنگ کے گزشتہ شماروں میں ہم کئی مفت اور بہترین اینٹی وائرس پروگرامز کا جائزہ لے چکے ہیں۔ اگر ایسی کوئی تحریر آپ کی نظر سے نہیں گزری تو کمپیوٹنگ کی ویب سائٹ پر موجود ''ڈاؤن لوڈز'' کے سیکشن میں تلاش کریں۔

ونڈوز ڈیفینڈر کو غیر فعال کرنے کے لیے Run کھول لیں۔ اس کے لیے آپ Win+R کا بٹن دبا سکتے ہیں۔

رن کھل جائے تو اس میں گروپ پالیسی ایڈیٹر کھولنے کے لیے gpedit.msc لکھ کر اینٹر پریس کر دیں۔



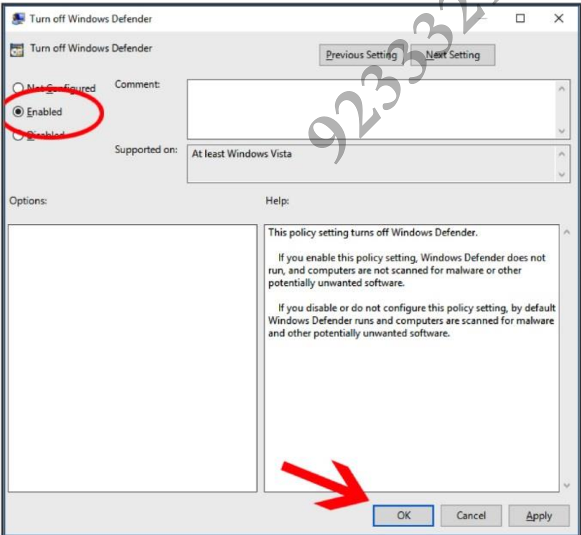
گروپ پالیسی ایڈیٹر کھل جائے تو اس میں درج ذیل مقام پر آ جائیں:



Computer Configuration → Administrative Templates → Windows Components → Windows Defender

یہاں Turn of Windows Defender پر ڈبل کلک کر کے اس کی پراپرٹیز کھول لیں۔

ونڈو کھل جائے تو یہاں موجود Enabled کے ساتھ چیک باکس کو چیک لگا کر او کے کر دیں۔



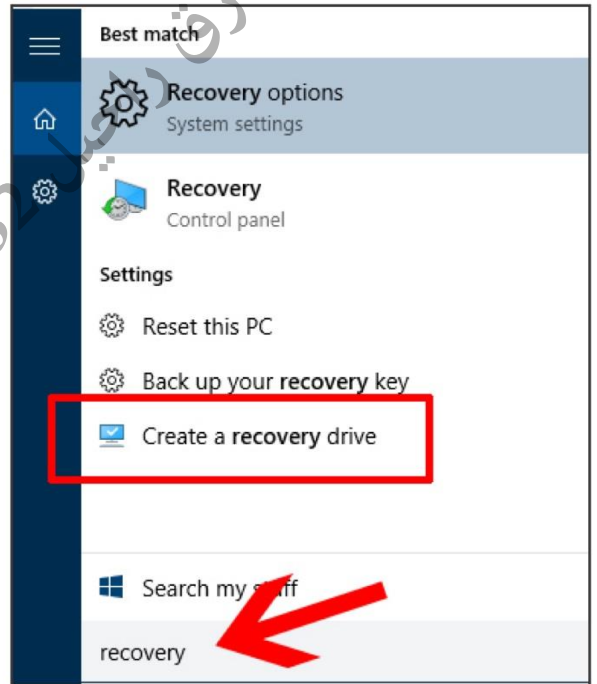
اب ونڈوز ڈیفینڈر سے جان چھڑانے کے لیے بس پی سی کو ری اسٹارٹ کرنے کی ضرورت ہے۔

ونڈوز 10 ریکوری ڈرائیو بنائیں

سسٹم میں کسی خرابی کی صورت میں ریکوری ڈرائیو انتہائی کارآمد ثابت ہوتی ہے۔ جب ونڈوز خراب ہوجائے اور سسٹم چل نہ پا رہا ہو تو اس ریکوری ڈرائیو سے اسے ٹھیک کیا جاسکتا ہے۔ کمپیوٹنگ کے گزشتہ شمارے میں آپ نے پڑھا ہو گا کہ ونڈوز 10 میں کس طرح پاس ورڈ ری سیٹ ڈسک بنائی جاتی ہے، آیئے اس بار آپ کو بتاتے ہیں کہ ونڈوز 10 میں کس طرح ریکوری ڈرائیو بنائی جاتی ہے۔ یہ کام بہت ہی آسان ہے، اس کے لیے کسی اضافی سافٹ ویئر کی ضرورت نہیں پڑتی کیونکہ یہ فیچر ونڈوز 10 میں پہلے سے موجود ہے۔

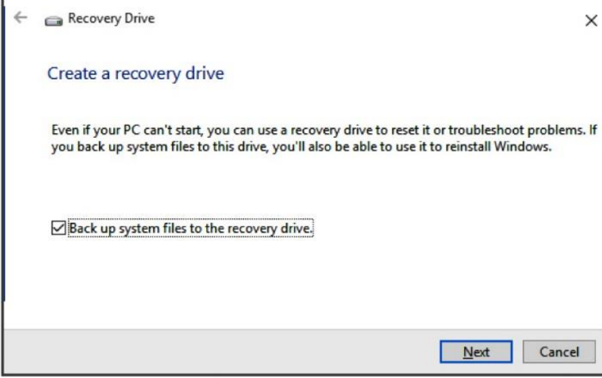
اس کام کے آغاز کے لیے اسٹارٹ بٹن پر کلک کرتے ہوئے سرچ بار میں Recovery ٹائپ کریں۔

ونڈوز چند سیکنڈز میں Create a recovery drive کو تلاش کر



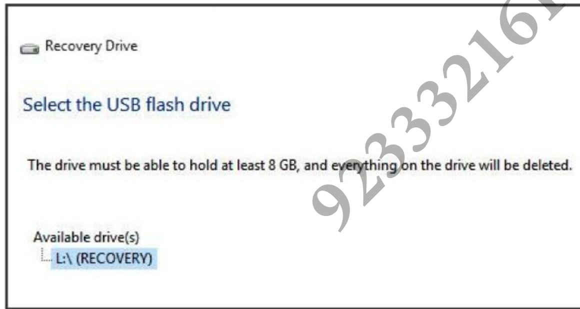
کے سامنے پیش کردے گی، اس پر کلک کردیں۔ ریکوری ڈرائیو کھل جائے، یہاں آپ دیکھ سکتے ہیں کہ ریکوری ڈرائیو میں سسٹم فائلز کو بیک اپ کرنے کا آپشن بھی دستیاب ہے اور یہ بھی بتایا جارہا ہے کہ ونڈوز میں کسی خرابی کی صورت میں اس ریکوری ڈرائیو سے آپ باآسانی ونڈوز کو ری اسٹور کرسکتے ہیں، اس لیے اس آپشن کو چیک لگا رہنے دیں۔

ظاہر ہے ریکوری ڈرائیو بنانے کے لیے آپ کو ایکسٹرنل ڈرائیو جیسے کہ یو ایس



بی فلیش ڈرائیو یا پاس پورٹ ڈرائیو کی ضرورت ہوگی۔ اگر آپ سسٹم فائلز کو بھی بیک اپ کرنا چاہتے ہیں تو آپ کو ایک بڑی اسٹوریج والی ڈیوائس درکار ہوگی، ورنہ چار سے آٹھ جی بی کی فلیش ڈرائیو کافی ہے، یوں سمجھ لیں کہ بتیس بٹ آپریٹنگ سسٹم کے لیے چار جی بی جبکہ چونسٹھ بٹ کے لیے آٹھ جی بی اسپیس کی حامل ڈرائیو درکار ہوتی ہے۔ لیکن اس ڈرائیو کو بھی پہلے خالی ضرور کرلیں کیونکہ اس عمل کے دوران اسے فارمیٹ کردیا جائے گا۔

نیکسٹ کے بٹن پر کلک کریں تو اگلے مرحلے پر سسٹم میں لگی ایکسٹرنل ڈرائیو کو منتخب کرنے کا کہا جائے گا۔



اگلے مرحلے پر متنبہ کیا جائے گا کہ آپ کی ڈرائیو میں موجود تمام ڈیٹا فارمیٹ ہوجائے گا، اس لیے پہلے اسے بیک اپ ضرور کرلیں۔ اگر آپ ریکوری ڈرائیو بنانے کے لیے تیار ہیں تو نیچے موجود Create کے بٹن پر کلک کردیں۔

اگلے مرحلے پر فائلز کاپی کرنے کا سلسلہ شروع ہوجائے گا۔

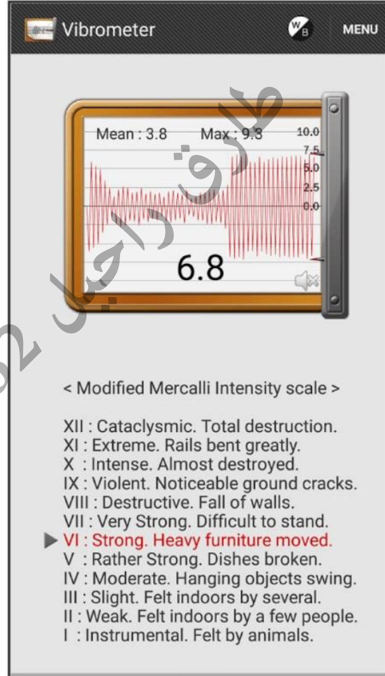
جب ریکوری ڈرائیو بنانے کا کام مکمل ہوجائے گا تو بتا دیا جائے گا کہ The recovery drive is ready۔

اب اگر خدانخواستہ کبھی آپ کی ونڈوز 10 چلنے سے قاصر ہو تو اس ڈرائیو کو پلگ کرکے سسٹم کو بوٹ کریں اور اس کی مدد سے ونڈوز کو بحال کرلیں۔

اپنے اینڈرائیڈ فون سے زلزلے کی شدت پیمائش کریں اور زلزلوں سے فوری آگاہ رہیں

8 اکتوبر کو برپا ہونے والے زلزلے سے پاکستان کے شمالی علاقے کے بعض شہر زبردست تباہی سے دوچار ہوئے ہیں۔ اس زلزلے کی شدّت ریکٹر اسکیل پر 7.8 ریکارڈ کی گئی ہے۔ بہت سے ذہنوں میں یقیناً یہ سوال اُبھرا ہوگا کہ زلزلے کی شدّت کی پیمائش کس طرح کی جاتی ہے اور ریکٹر اسکیل یا ریکٹر پیمانہ کیا شے ہے؟ ریکٹر اسکیل کی تعریف اُردو وکی پیڈیا پر کچھ یوں موجود ہے:

''زلزلے کی آمد، سمت اور زلزلوں کی شدّت معلوم کرنے کے لئے ماہرینِ ارضیات جو آلہ استعمال کرتے ہیں وہ سیسموگراف (Seismograph) کہلاتا ہے۔ اس آلہ کے ذریعے زمین میں آنے والے ارتعاش کو ریکارڈ کیا جاتا تھا۔ یہ آلہ بھی پنڈولم کی مدد ہی سے کام کرتا تھا۔ اس پنڈولم کے ساتھ ایک قلم بھی منسلک کی گئی تھی جو منسلک پیپر رول پر ایک لکیر کی صورت میں نشان بناتی چلی جاتی تھی۔ جب بھی زلزلے کی لہر اُٹھتی تو پنڈولم میں بھی ارتعاش پیدا ہوتا یوں پیپر رول پر ارتعاشی لہر کی نشاندہی ہوجاتی۔ جس پر زلزلے کی شدت کو 1 سے لے کر 12 درجے تک ناپا جاسکتا ہے۔ اس پیمائش کو ریکٹر اسکیل (Richter Scale) کا نام دیا جاتا ہے۔ ریکٹر اسکیل پر 1 سے لے کر 5 درجے تک کی پیمائش ہلکے سے درمیانی شدت کے زلزلے کو ظاہر کرتی ہے جبکہ 6 سے لے کر 12 تک کے درجے درمیانی شدت سے انتہائی شدت والے زلزلے کو ظاہر کرتے ہیں۔''



Alarm level

No Beep
1.0+
2.0+
3.0+
4.0+
5.0+
6.0+
7.0+
8.0+
9.0+

چونکہ زلزلے کثرت سے آتے رہتے ہیں لیکن ان کی شدت کم ہوتی ہے، لوگ انھیں محسوس نہیں کرتے اس لیے آپ ان سے بے خبر رہتے ہیں اور میڈیا میں بھی ان کی کوئی خبر نہیں ہوتی۔ اگر آپ زلزلوں کو ماپنا چاہتے ہیں تو اس کے لیے سیسموگراف درکار ہوگا لیکن اگر آپ کے پاس اینڈرائیڈ فون موجود ہے تو ''وائبرومیٹر'' ایپلی کیشن سے آپ زلزلے کی شدت ناپ سکتے ہیں۔ ایپلی کیشن کے اچھے نتائج حاصل کرنے کے لیے آپ کو اس کے کام کرنے کے طریقہ کار کو سمجھنا ہوگا۔ اس کی انسٹالیشن کے بعد فون کا ہموار اور ساکن سطح پر موجود ہونا زلزلے کی زیادہ درست پیمائش دیتا ہے۔ اگرچہ اس کی پیمائش سو فیصد درست اور سیسموگراف آلے جیسی نہیں ہوتی لیکن پھر بھی کسی آلے کے بغیر زلزلے کی شدت کو ماپنا اس ایپلی کیشن نے ممکن کر دیا ہے۔ اس میں الارم بھی لگایا جاسکتا ہے جو زلزلے کے وقت فوراً خبردار کرے گا۔

bit.ly/vibrometer

ریکٹر اسکیل (Richter scale)

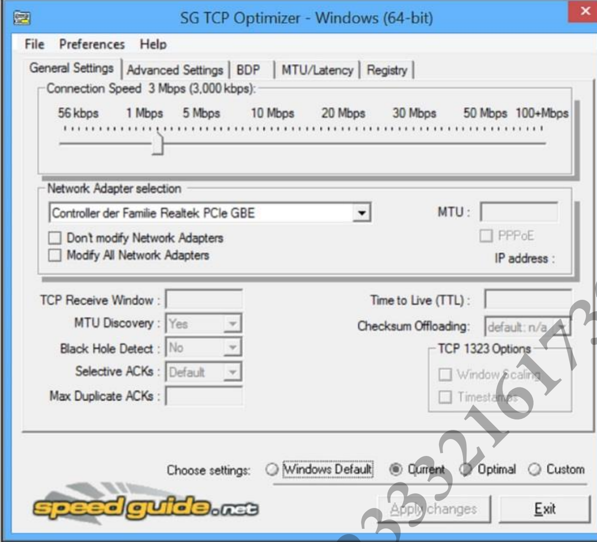
زلزلے کی شدت	زلزلے کا اثر	زلزلے کے واقعات
2.0 سے کم	اس شدت کے زلزلے محسوس نہیں کئے جاسکتے، یہ بہت عام ہیں۔	ہر روز تقریباً 8000 بار
2.0 تا 2.9	محسوس نہیں کئے جاسکتے لیکن زلزلہ پیما پر ریکارڈ ہو جاتے ہیں	ہر روز تقریباً 1000 بار
3.0 تا 3.9	محسوس کئے جاسکتے ہیں لیکن ان سے نقصان کا اندیشہ کم ہوتا ہے	ہر سال تقریباً 49000 بار
4.0 تا 4.9	اکثر اشیاء کو ہلتے ہوئے دیکھا جاسکتا ہے، چنگاڑتی ہوئی آواز سنائی دے سکتی ہے۔ بڑے نقصان کا اندیشہ کم ہوتا ہے	ہر سال تقریباً 6200 بار
5.0 تا 5.9	غیر معیاری تعمیر شدہ یا خستہ حال عمارتوں کو شدید نقصان پہنچ سکتا ہے، تباہی زلزلے کے مرکز پر زیادہ ہوتی ہے	ہر سال تقریباً 800 بار
6.0 تا 6.9	زلزلے کے مرکز سے ایک سو میل دور تک گنجان آبادیوں کو شدید مالی و جانی نقصان پہنچ سکتا ہے	ہر سال تقریباً 120 بار
7.0 تا 7.9	زلزلے کی شدت سینکڑوں میل دور تک محسوس کی جاتی ہے اور یہ زیادہ دور تک شدید جانی اور مالی نقصان کا باعث بنتے ہیں	ہر سال تقریباً 18 بار
8.0 تا 8.9	زلزلے کے مرکز سے ہزاروں میل دور تک زلزلے کا اثر محسوس کیا جاسکتا ہے۔ یہ عظیم تباہی پھیلاتے ہیں	ہر سال تقریباً ایک
9.0 تا 9.9	ہزاروں میل دور تک انتہائی شدید تباہی پھیلاتے ہیں	تقریباً ہر 20 سال بعد ایک
10+	اس اسکیل کا زلزلہ آج تک ریکارڈ نہیں کیا گیا	انسانی تاریخ میں آج تک نہیں

مفت ڈاؤن لوڈز

انٹرنیٹ کی دنیا سے کارآمد سافٹ ویئر

65%

انٹرنیٹ کی مکمل تیز رفتار حاصل کریں

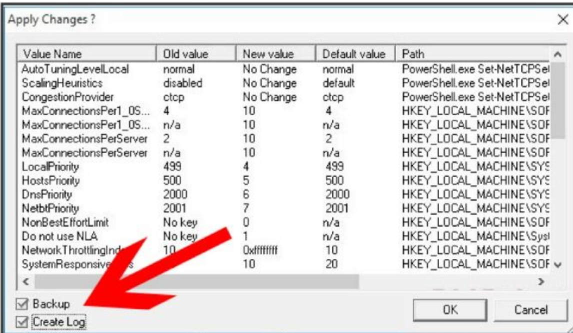


چاہے آپ کے پاس کتنا ہی تیز رفتار انٹرنیٹ موجود ہو آپ اس کی اصل رفتار استعمال نہیں کر پاتے۔ دراصل آپ کے انٹرنیٹ کی رفتار کو ونڈوز آپریٹنگ سسٹم کی سیٹنگز متاثر کرتی ہیں۔ کچھ TCP/IP سیٹنگز کے بعد اپنے انٹرنیٹ کو پہلے سے زیادہ قابل اعتبار بنایا جا سکتا ہے اور اس کی ممکنہ تیز اسپیڈ بھی حاصل کی جا سکتی ہے۔ ان سیٹنگز کو مینوئلی یعنی خود بھی کیا جا سکتا ہے اور ان کے لیے کوئی سافٹ ویئر بھی استعمال کیا جا سکتا ہے۔ اگر آپ ونڈوز 10 میں یہ تجربہ کرنا چاہیں تو اس کے لیے ''ایس جی، ٹی سی پی آپٹمائزر ٹول'' مفت دستیاب ہے۔ یہ ٹول ''اسپیڈ گائیڈ اِنکارپوریشن'' کا بنایا ہوا ہے۔

SG TCP Optimizer ایک پورٹ ایبل ٹول ہے یعنی اسے استعمال کرنے کے لیے انسٹال کرنے کی بھی ضرورت نہیں۔ اسے ونڈوز 10 کے علاوہ ونڈوز 8 اور 8.1 پر بھی استعمال کیا جا سکتا ہے۔ اس کے کچھ فیچرز کے لیے ضروری ہوتا ہے کہ آپ کے پاس ایڈمنسٹریٹر اختیارات موجود ہوں، اس لیے اس پر رائٹ کلک کرتے ہوئے Run as administrator کے ذریعے اسے چلائیں۔

پروگرام کے سب سے نچلے حصے میں دیکھیں تو یہاں مختلف سیٹنگز موجود ہیں۔ عام صارفین یہاں سے Optimal منتخب کرتے ہیں۔ تاکہ سافٹ ویئر اپنے حساب سے ضرورت کی سیٹنگز کر دے۔ لیکن اگر آپ اس حوالے سے کچھ مہارت رکھتے ہیں تو Custom کو منتخب کرتے ہوئے ساری سیٹنگز کے ساتھ خود بھی چھیڑ چھاڑ کر سکتے ہیں۔ سارے کام مکمل ہونے کے بعد Apply changes کے بٹن پر کلک کریں۔ جو سیٹنگز یہ پروگرام بدلنے جا رہا ہوگا اگلے مرحلے پر ان کی تفصیل دکھائی جائے گی۔ کی گئی تبدیلیوں کو یاد رکھنے کے لیے آپ یہاں Create Log کے آپشن کو چیک لگا دیں اس کے علاوہ Backup کے ساتھ بھی چیک لگا دیں تو کی گئی تمام سیٹنگز سے پہلے بیک اپ بھی لے لیا جائے گا تاکہ پرانی سیٹنگز پر باآسانی واپس جایا جا سکے۔ یاد رہے کہ کچھ سیٹنگز کو تبدیلی کے بعد ری اسٹارٹ بھی درکار ہوتا ہے۔

www.speedguide.net/downloads.php



Apply Changes ?

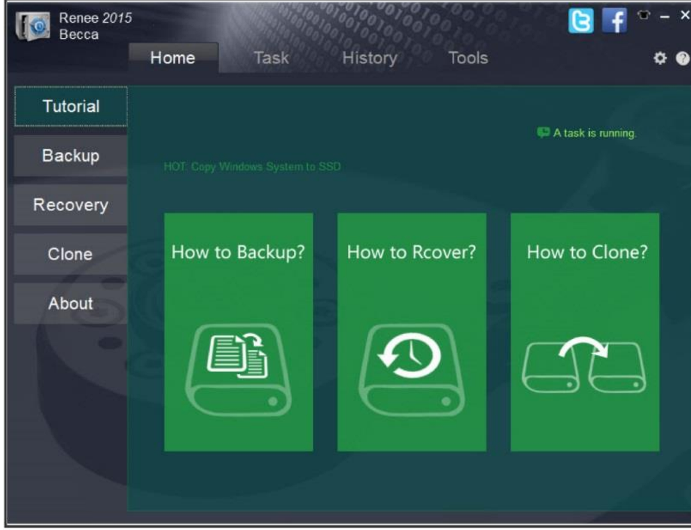
Value Name	Old value	New value	Default value	Path
AutoTuningLevelLocal	normal	No Change	normal	PowerShell.exe Set-NetTCPSe
ScalingHeuristics	disabled	No Change	default	PowerShell.exe Set-NetTCPSe
CongestionProvider	ctcp	No Change	ctcp	PowerShell.exe Set-NetTCPSe
MaxConnectionsPer1_0S...	4	10	4	HKEY_LOCAL_MACHINE\SOF
MaxConnectionsPer1_0S...	n/a	10	n/a	HKEY_LOCAL_MACHINE\SOF
MaxConnectionsPerServer	2	10	2	HKEY_LOCAL_MACHINE\SOF
MaxConnectionsPerServer	n/a	10	n/a	HKEY_LOCAL_MACHINE\SOF
LocalPriority	499	4	499	HKEY_LOCAL_MACHINE\SYS
HostsPriority	500	5	500	HKEY_LOCAL_MACHINE\SYS
DnsPriority	2000	6	2000	HKEY_LOCAL_MACHINE\SYS
NetbtPriority	2001	7	2001	HKEY_LOCAL_MACHINE\SYS
NonBestEffortLimit	No key	0	n/a	HKEY_LOCAL_MACHINE\SOF
Do not use NLA	No key	1	n/a	HKEY_LOCAL_MACHINE\Syst
NetworkThrottlingInd...	10	0xffffffff	10	HKEY_LOCAL_MACHINE\SOF
SystemResponsive...		10	20	HKEY_LOCAL_MACHINE\SOF

Backup

Create Log

OK Cancel

”سسٹم بیک اپ کا بادشاہ“ .... آزما کر دیکھیں



کبھی بھی اس غلط فہمی میں مت رہیں کہ آپ کا سسٹم کبھی دھوکا نہیں دے گا۔ یہ ایسے وقت میں دھوکا دیتا ہے جب ہمیں اس کی امید بھی نہیں ہوتی۔ یہی وجہ ہے کہ ہم بیک اپ پر بہت زور دیتے ہیں۔ اپنی اہم فائلوں بلکہ مکمل سسٹم کا بیک اپ آپ کے پاس ضرور موجود ہونا چاہیے۔ Reneelab کے مطابق اس وقت Renee Becca دنیا کا سب سے بہترین ڈیٹا بیک اپ سافٹ ویئر ہے۔ یقیناً آپ اسے آزمانے کے بعد ہی اس بات کی تصدیق کرسکتے ہیں تو آیئے اس پر ایک نظر ڈالتے ہیں۔

”رینی بیکا“ مفت اور کمرشل ورژن دونوں صورتوں میں دستیاب ہے۔ مفت ورژن کو استعمال کرنے کے لیے آپ کو اپنا ای میل ایڈریس دینا پڑتا ہے تاکہ Key موصول کرسکیں۔ اس کے اندراج کے بعد اس کے تمام فیچرز استعمال کرنے کے لیے کھل جاتے ہیں۔

اپنے پہلے استعمال پر یہ مکمل ٹیوٹوریئل دکھاتا ہے کہ کس طرح اسے استعمال کیا جاتا ہے۔ اس پروگرام کے ذریعے آپ ڈیٹا بیک اپ کرسکتے ہیں، پہلے سے بیک اپ شدہ ڈیٹا کو ری اسٹور کرسکتے ہیں اور ڈیٹا کلون کرتے ہوئے ایک ڈرائیو سے دوسری ڈرائیو پر محفوظ کرسکتے ہیں۔

کلون (Clone)

اس کے کلون فیچر کے ذریعے مکمل ہارڈ ڈسک، پارٹیشن یا سسٹم کا کلون بنایا جا سکتا ہے یعنی بالکل اُسی جیسی کاپی بنائی جاسکتی ہے جسے کسی دوسرے سسٹم یا اسی سسٹم پر کسی خرابی کی صورت میں ری اسٹور بھی کیا جاسکتا ہے۔ اس فیچر کو استعمال کرنے کے لیے ضروری ہے کہ جس ڈرائیو کا کلون بنایا جارہا ہو اور جس ڈرائیو میں اس کلون کو محفوظ کرنا ہے دونوں بیک وقت دستیاب ہوں۔

www.reneelab.com/data-backup

بیک اپ (Backup)

ڈیٹا بیک اپ کی بات کی جائے تو سسٹم بیک اپ یعنی جس پارٹیشن میں ونڈوز موجود ہو کا بیک اپ بنایا جاسکتا ہے۔

ڈسک/ پارٹیشن بیک اپ کے ذریعے سسٹم میں موجود کسی بھی ہارڈ ڈرائیو یا پارٹیشن کا بیک اپ بنایا جاسکتا ہے۔

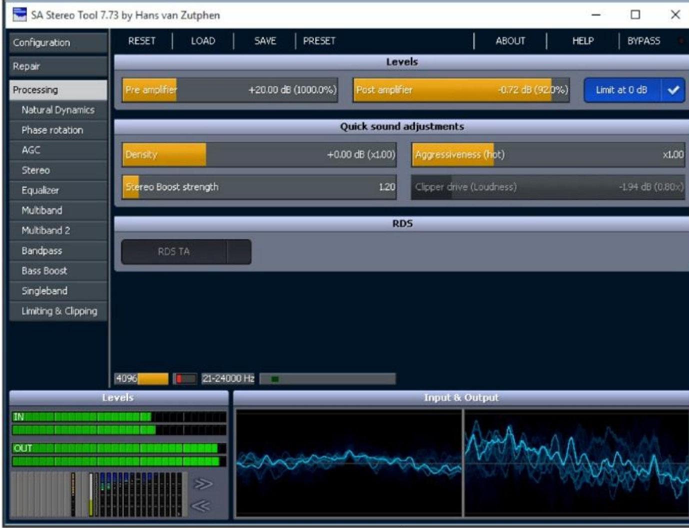
فائل بیک اپ کے ذریعے انفرادی فائلز اور فولڈرز کو بیک اپ کرنے کی سہولت بھی موجود ہے۔



ریکوری (Recovery)

ریکوری کے ذیل میں سسٹم ریکوری، ڈسک/ پارٹیشن ریکوری اور فائل ریکوری کے آپشنز موجود ہیں، لیکن انھیں استعمال کرنے کے لیے ضروری ہے کہ پہلے آپ اس پروگرام کے ذریعے بیک اپ بنائیں تاکہ اس بیک اپ سے یہ کام انجام دے سکے۔

پی سی پر گانے سننے کا لطف دوبالا کریں



کمپیوٹر یا لیپ ٹاپ پر کام کرتے ہوئے بیک گراؤنڈ میں موسیقی سے لطف اندوز ہونا سبھی کو پسند ہوتا ہے۔ اکثر لوگ اونچی آواز میں گانے سننے کے لیے اضافی اسپیکرز استعمال کرتے ہیں تو کچھ لوگ ہیڈفونز استعمال کرنا پسند کرتے ہیں جبکہ کچھ لوگ لیپ ٹاپ میں لگے اسپیکرز پر ہی اکتفا کر لیتے ہیں۔ آپ نے یقیناً نوٹ کیا ہوگا کہ لیپ ٹاپ یا سسٹم میں موجود اسپیکر سے گانوں کی آواز ہیڈفونز کے مقابلے میں کم آتی ہے۔ اس لیے لوگ سمجھتے ہیں کہ میوزک سے صحیح معنوں میں لطف اندوز ہونے کے لیے اچھا ہیڈفون موجود ہونا ضروری ہے۔ آپ کو پتا ہونا چاہیے کہ میڈیا پلیئر میں ایک اچھے پلگ اِن کے ذریعے میوزک کو نہ صرف اونچا بلکہ صاف اور شفاف بنایا جاسکتا ہے۔ اس طرح میوزک سننے کا لطف دوبالا ہوجاتا ہے۔

جس پلگ اِن کا ذکر ہم کررہے ہیں اس کا نام ''اسٹیریو ٹول'' ہے۔ اگر آپ اچھے معیار کی موسیقی سے لطف اندوز ہونا چاہتے ہیں تو ہماری ہدایت کے مطابق اس پلگ اِن کا استعمال کریں اور فرق دیکھیں۔

اسٹیریو ٹول دیکھنے میں تو آپ کو 90 کی دہائی کا کوئی پروگرام نظر آئے گا لیکن شکل چھوڑیے جناب اس کی کارکردگی پر توجہ دیں۔ یہ نہ صرف کم آواز والے گانوں کو اونچا کردیتا ہے بلکہ پرانی سی ڈیز میں موجود گانوں کی چھوٹی موٹی خرابیاں دُور کرتے ہوئے انھیں سننے کے قابل بنادیتا ہے۔

اسٹیریو ٹول کئی مختلف صورتوں میں دستیاب ہے۔ اس کا DSP پلگ اِن وِن ایمپ میڈیا پلیئر کے لیے، VST پلگ اِن وی ایس ٹی ہوسٹس کے لیے جبکہ ویسے ہی انسٹالیشن کے لیے اسٹینڈ الون انسٹالر کی صورت میں بھی موجود ہے۔ وِن ایمپ میڈیا پلیئر کے ساتھ اس کی کارکردگی شاندار ہے اور ہم بھی اسے وِن ایمپ کے ساتھ استعمال کرنے کا مشورہ دیں گے۔ اگر آپ کے پاس وِن ایمپ میڈیا پلیئر موجود نہیں تو سب سے پہلے اسے درج ذیل ربط سے ڈاؤن لوڈ کرکے انسٹال کرلیں:

bit.ly/winampfull

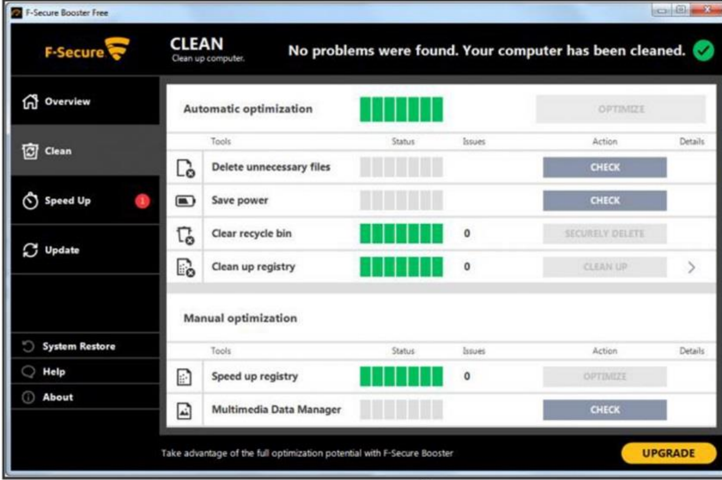
وِن ایمپ کی انسٹالیشن کے بعد اسٹیریو ٹول کا پلگ اِن بھی درج ذیل ربط سے ڈاؤن لوڈ کرکے انسٹال کرلیں:

stereotool.com/download

اس پلگ اِن کو زیادہ کنفگریشن درکار نہیں، یہ خود بخود سسٹم کی آڈیو سیٹنگز کو درست کردیتا ہے لیکن اگر آپ اس کے ساتھ مزید چھیڑ چھاڑ کرنا چاہیں تو یہ بھی ممکن ہے۔ پلگ اِن انسٹال ہونے کے بعد خود بخود اپنے ساتھ ساتھ وِن ایمپ میڈیا پلیئر کو بھی کھول لے گا۔ اب آپ اس میں کوئی گانا چلائیں اور فرق دیکھیں۔ اگر آپ فرق کو واضح طور پر محسوس کرنا چاہیں تو اسٹیریو ٹول پر سب سے اوپر دائیں طرف موجود BYPASS کے آپشن پر کلک کریں، یہ پلگ اِن کام کرنا بند کردے گا اور گانا پرانی سیٹنگز پر چلے گا۔ اسی آپشن پر کلک کرتے ہوئے آپ دوبارہ پلگ اِن کو فعال کرسکتے ہیں۔



اپنے پی سی کو اس کی اصل کارکردگی پر بحال کریں



کمپیوٹنگ میں آپ نے ''ایف سکیور بوسٹر اینڈرائیڈ ایپ'' کے بارے میں پڑھا ہوگا، لیجیے اب یہ شاندار پروگرام کمپیوٹر کے لیے بھی پیش کر دیا گیا ہے۔ یقیناً آپ جانتے ہوں گے کہ ونڈوز استعمال کے ساتھ ساتھ سست ہوتی جاتی ہے، دراصل اس میں جمع ہونے والا کچرا اس کی رفتار پر اثر انداز ہوتا ہے۔ سسٹم کی صفائی کے لیے آپ کو چاہیے ہوتا ہے ایک کلینر پروگرام۔ اس حوالے سے آپ نے بڑے بڑے نام سنے ہوں گے لیکن کیوں نا اب کی بار ''ایف سکیور'' کے اس نئے پروگرام کو موقع دیا جائے؟ ایف سکیور بوسٹر فار پی سی آپ کے سسٹم کی مجموعی کارکردگی کو بہتر بناتا ہے۔ یہ سسٹم میں موجود پروگرامز کی باقیات اور غیر ضروری فائلز کو حذف کرتا ہے، ونڈوز رجسٹری کی خرابیاں درست کرتا ہے، لیپ ٹاپ صارفین کے لیے ایسا پاور پلان مرتب کرتا ہے جس سے توانائی کی بچت ہو سکے، ری سائیکل بِن میں موجود فائلز کو اس طرح ٹھکانے لگاتا ہے کہ کوئی انھیں واپس حاصل نہ کر سکے، ونڈوز کی سروسز کو درست کرتا ہے اس کے علاوہ سسٹم میں انسٹال سافٹ ویئر اور ڈرائیورز کو بھی اپ ڈیٹ کر سکتا ہے۔

اس کی انسٹالیشن کے بعد جب آپ اسے چلائیں گے تو یہ فوراً ہی سسٹم کو اسکین کرنا شروع کر دے گا تا کہ ان وجوہات کو تلاش کر سکے جن کی وجہ سے سسٹم سست ہو رہا ہے یا درست طریقے سے کام نہیں کر پا رہا۔ جائزے کے اس عمل میں کچھ وقت یعنی دس سے پندرہ منٹس لگ سکتے ہیں۔

ایف سکیور کے اگر انٹرفیس یعنی شکل پر نظر ڈالیں تو اسے تین حصوں کلین، اسپیڈ اپ اور اپ ڈیٹ میں تقسیم کیا گیا ہے۔

کلین (Clean)

اگر آپ سسٹم میں موجود فالتو فائلز سے نجات حاصل کرنا چاہتے ہیں تو کلین کے حصے میں آئیں۔ یہاں ''آپٹمائز'' کے بٹن پر کلک کر کے آپ خودکار طریقے سے سسٹم کی صفائی کر سکتے ہیں اور اگر چاہیں تو خود مینوئلی بھی فائلز کو حذف کر سکتے ہیں۔

اسپیڈ اپ (Speedup)

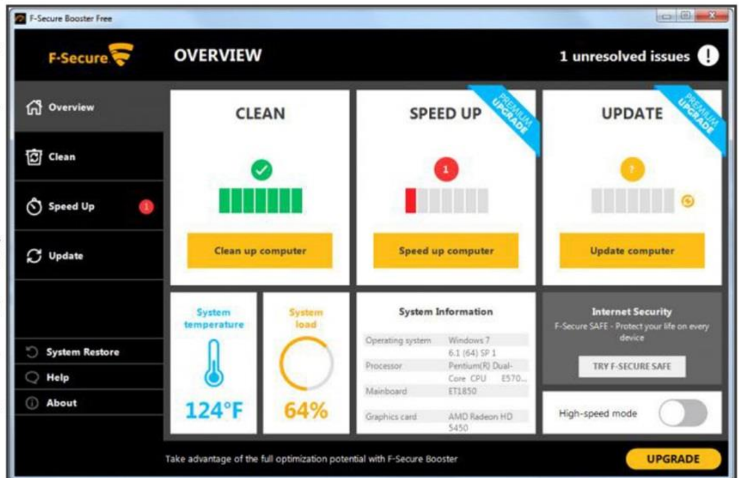
اگر آپ کو محسوس ہو کہ سسٹم بہت سست پڑ رہا ہے، اس کی کارکردگی پہلے جیسی نہیں رہی تو اسپیڈ اپ کے حصے میں آ جائیں۔ اس کے ذریعے آپ غیر ضروری استعمال ہونے والی ریسورسز کا خاتمہ کر سکتے ہیں۔

اپ ڈیٹ (Update)

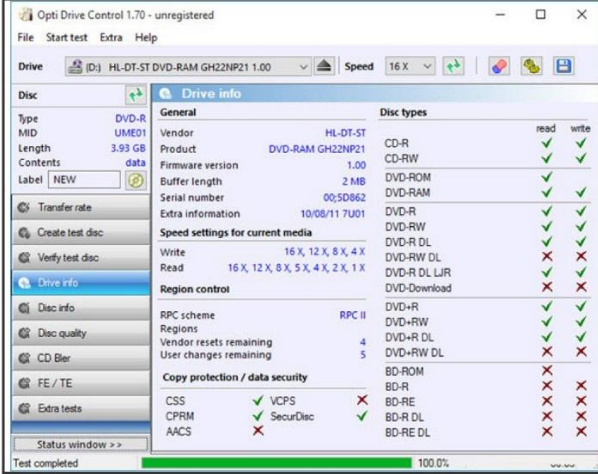
اگر آپ انسٹال پروگرامز اور ڈرائیورز کو اپ ڈیٹ کرنے کا ارادہ رکھتے ہیں تو ''اپ ڈیٹ'' کے حصے میں آنا پڑے گا۔

غرض ایف سکیور پروگرام میں ایک سست پڑتے ونڈوز پی سی کی درستگی کے لیے تمام ٹولز موجود ہیں۔

bit.ly/fsecure-booster

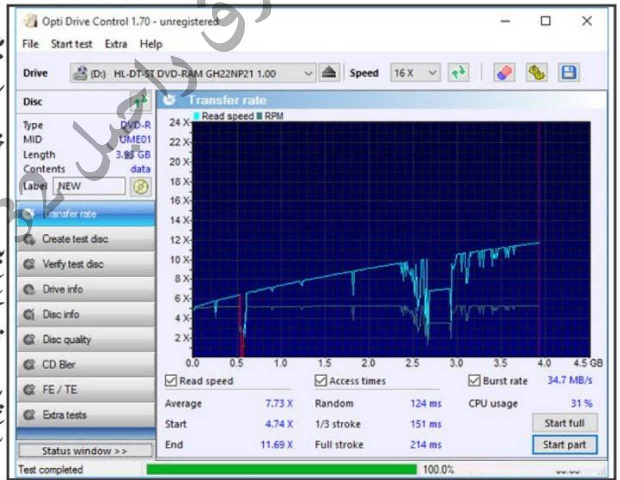


سی ڈی یا ڈی وی ڈی ڈرائیو کی درستگی چیک کریں



یو ایس بی فلیش ڈرائیوز کی آمد نے آپٹیکل ڈِسک ڈرائیوز (ODD) کا استعمال انتہائی محدود کر دیا ہے۔ آپٹیکل ڈِسک ڈرائیو جسے ہمارے ہاں عموماً سی ڈی ڈرائیو یا ڈی وی ڈی ڈرائیو کہا جاتا ہے، کو اب بمشکل ونڈوز کی انسٹالیشن کے وقت ہی استعمال کیا جاتا ہے۔ یہی وجہ ہے کہ کمپیوٹر میں لگی آپٹیکل ڈِسک ڈرائیو فارغ رہ رہ کر ناکارہ ہوجاتی ہے۔ اس کے بعد اگر کبھی کوئی سی ڈی یا ڈی وی ڈی بنانے کی ضرورت پڑے تو یہ ڈرائیو بجائے ڈیٹا درست طریقے سے ڈی وی ڈی پر ڈالنے کے اُسے خراب کر دیتی ہے۔

اگر آپ بھی اس مسئلے کا شکار ہیں تو اپنا وقت اور ڈی وی ڈیز کو ضائع ہونے سے بچا سکتے ہیں۔ اس کے لیے آپ کو ''آپٹی ڈرائیو کنٹرول'' سافٹ ویئر درکار ہوگا جو آپ کی آپٹیکل ڈِسک ڈرائیو کو چیک کرکے بتا سکتا ہے کہ آیا یہ درست طریقے سے کام کر رہی ہے یا نہیں۔ کیونکہ ایسا بھی ممکن ہے کہ آپ سی ڈی یا ڈی وی ڈی ہی خراب استعمال کر رہے ہوں، اس لیے آپٹیکل ڈِسک ڈرائیو کو چیک کر لینا انتہائی ضروری ہے۔



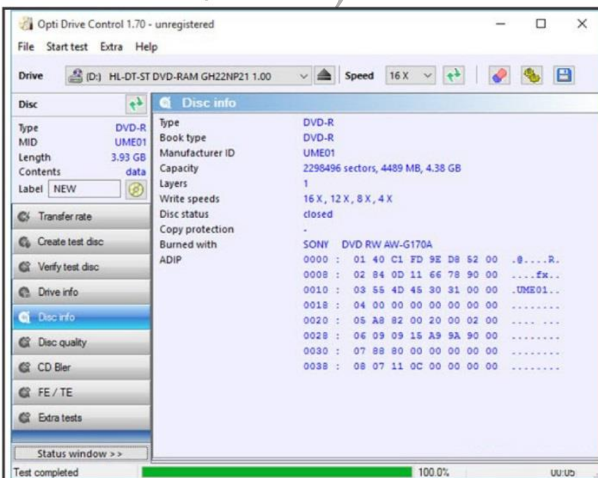
Opti Drive Control سافٹ ویئر ویسے تو ونڈوز 7 کے لیے بنایا گیا ہے لیکن یہ ونڈوز 8 اور 10 پر بھی درست طریقے سے کام کرتا ہے۔

آپٹی ڈرائیو کنٹرول کو انسٹال کرنے کی بھی ضرورت نہیں پڑتی کیونکہ یہ پورٹ ایبل صورت میں دستیاب ہے۔ اسے استعمال کرنے کے لیے آپ کو ایک عدد خالی سی ڈی یا ڈی وی ڈی درکار ہوگی، جسے ڈرائیو میں لگا کر اس سافٹ ویئر کے ذریعے ٹیسٹ کا آغاز ہوگا۔ سی ڈی پر نہ صرف ڈیٹا ڈالا جائے گا بلکہ اس سے پی سی میں کاپی کرکے بھی دیکھا جائے گا تاکہ ٹرانسفر ریٹ کا پتا چل سکے۔

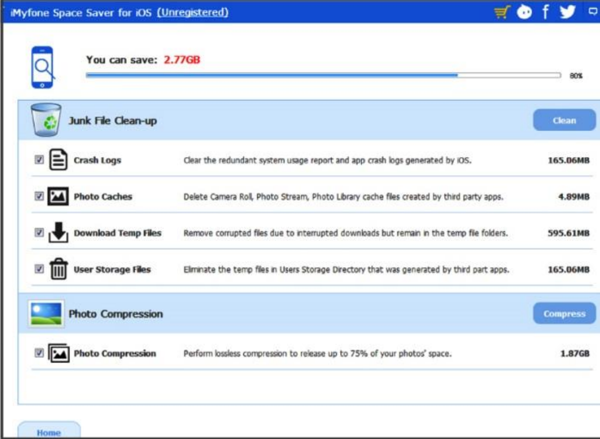
آپ کا سی ڈی روم سی ڈی یا ڈی وی ڈی کو پڑھ تو پا رہا ہے لیکن اس میں موجود ڈیٹا کاپی نہیں کر پا رہا تو اس صورت میں بھی یہ سافٹ ویئر انتہائی کارآمد ثابت ہوگا۔ اس مسئلے کا شکار اکثر لوگ سمجھتے ہیں کہ ان کی ڈی وی ڈی خراب ہوچکی ہے لیکن دراصل مسئلہ آپٹیکل ڈِسک ڈرائیو میں ہوتا ہے۔

ٹیسٹ کے دوران استعمال ہونے والی خالی سی ڈی یا ڈی وی ڈی کے بارے میں یہ سافٹ ویئر بہت کارآمد معلومات بھی دِکھاتا ہے جس سے آپ جان سکتے ہیں کہ آپ کی آپٹیکل ڈرائیو کو کسی مخصوص برانڈ کی سی وی ڈی کے ساتھ مسئلہ تو نہیں۔ اگر سی ڈی اور ڈی وی ڈی استعمال کرنا آپ کا روزمرہ کا معمول ہے تو یہ پروگرام ضرور استعمال کریں۔ یاد رہے کہ یہ پروگرام صرف مسئلے کی نشاندہی کر سکتا ہے اسے ٹھیک نہیں۔

www.optidrivecontrol.com

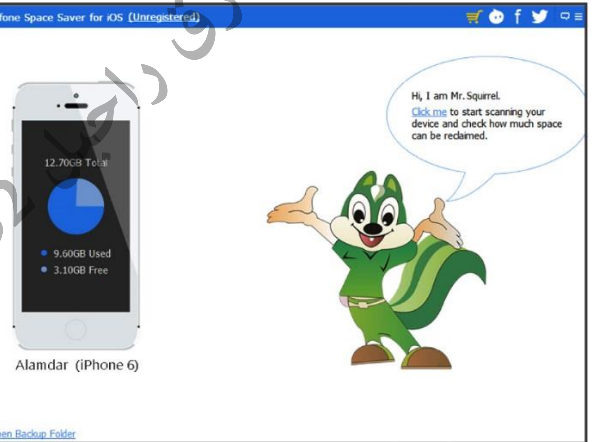


آئی فون سے فالتو فائلز حذف کرکے خالی اسپیس حاصل کریں



اسمارٹ فون کئی کمپنیوں کے موجود ہیں لیکن جو اہمیت آئی فون کو حاصل ہے وہ کسی اور کو نہیں۔ ہر کسی کی خواہش ہوتی ہے کہ اس کے پاس ایک خوبصورت آئی فون موجود ہو۔ کسی خوشی کے موقعے پر اگر تحفے میں آئی فون ملے تو خوشی دوبالا ہو جاتی ہے۔ آئی فون کی خصوصیات، دلکشی یا یوں کہیں بھرم تو ہے لیکن قیمت بھی اسی حساب سے بہت اونچی ہے۔

جب آپ آئی فون خریدتے ہیں تو کوشش ہوتی ہے کہ اس کے تمام فیچرز سے بھرپور انداز میں لطف اندوز ہوں۔ اس لیے آپ اس میں اپنی ضرورت اور پسند کے مطابق ایپلی کیشنز اور گیمز انسٹال کرتے ہیں۔ مسئلہ اس وقت پیدا ہوتا ہے جب فون کی ڈرائیو میں اسپیس کم پڑنے لگے۔ اگر آپ آئی فون استعمال کرتے ہیں تو آپ کے پاس ''آئی مائی فون اسپیس سیور'' سافٹ ویئر بھی موجود



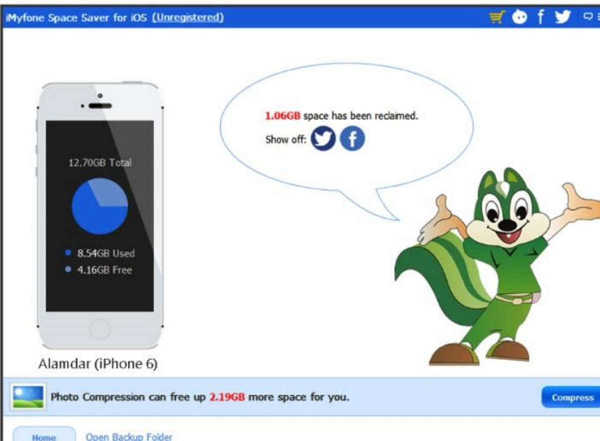
ہونا چاہیے۔ یہ پروگرام آئی فون، آئی پیڈ اور آئی پوڈ کی صفائی کرکے اس میں زیادہ سے زیادہ خالی گنجائش بنانے میں مدد دیتا ہے۔ اس صفائی میں یہ پروگرام فون میں جمع ہونے والی فالتو فائلز کو حذف کرتا ہے جبکہ فون میں موجود JPEG تصاویر کو کمپریس کرتا ہے۔

اس پروگرام کو استعمال کرنا بہت ہی آسان ہے۔ ونڈوز پی سی پر اس کی انسٹالیشن کے بعد اسے چلائیں، اپنے آئی فون کو یو ایس بی کیبل کے ذریعے پی سی سے جوڑیں۔ یہ پروگرام آپ کے فون کو پہچاننے کے بعد اس میں موجود خالی اور استعمال شدہ اسپیس کی تفصیل دِکھا دے گا۔ صفائی کے آغاز کے لیے گلہری کے کارٹون کردار کی ہدایت کے مطابق Click Me پر کلک کردیں۔

اگلے مرحلے پر دِکھایا جائے گا کہ کون کون سی فائلز جیسے کہ کیشے لاگز اور غیر ضروری عارضی فائلز حذف کرکے آپ کتنی اسپیس حاصل کرسکتے ہیں۔ اگر آپ انھیں حذف کرنے پر رضامند ہوں تو Clean کے بٹن پر کلک کردیں۔

آئی فون میں بہت اچھا کیمرہ نصب ہے اس لیے اس کے ذریعے بنائی گئی تصاویر کا حجم بھی بہت زیادہ ہوتا ہے جیسے کہ پانچ سے دس ایم بی کی ایک تصویر ہوتی ہے۔ یہ پروگرام تمام تصاویر کو بغیر کوالٹی متاثر کیے کمپریس کرسکتا ہے۔ مثلاً پانچ ایم بی کی تصویر کو ایک ایم بی میں سما سکتا ہے۔ اگرچہ اس کا کہنا ہے کہ تصاویر کا معیار متاثر نہیں ہوتا لیکن بجائے براہِ راست اسے استعمال کرنے کے تصاویر کو پہلے بیک اپ ضرور کرلیں، پھر اس کی مدد سے تصاویر کو کمپریس کرلیں۔ فون میں رکھنے کے لیے اور کسی سے شیئر کرنے کے لیے ان کمپریسڈ تصاویر کا معیار بھی بہت کافی ثابت ہوگا اس لیے پریشانی کی کوئی بات نہیں۔ یاد رہے کہ یہ پروگرام فون کی صفائی کرنے سے پہلے کسی قسم کا بیک اپ نہیں بناتا، لیکن چونکہ یہ صرف فالتو فائلز حذف کرتا ہے اس لیے کسی قسم کا کوئی مسئلہ نہیں ہوتا۔

imyfone.com/ios-space-saver



ونڈوز کو اپ ڈیٹ کرنا آسان بنائیں

تمام سافٹ ویئر اور ونڈوز میں دریافت ہونے والی خرابیوں کو درست کرنے کے لیے اور نئے فیچرز شامل کرنے کے لیے اپ ڈیٹس جاری کی جاتی ہیں۔ ونڈوز کی بات کی جائے تو اس کی اپ ڈیٹس بہت تواتر سے جاری ہوتی رہتی ہیں۔ زیادہ تر صارفین ان اپ ڈیٹس کو ونڈوز میں پہلے سے موجود ٹول ''ونڈوز اپ ڈیٹ'' کی مدد سے حاصل کرتے ہیں۔ ان اپ ڈیٹس کو سمجھنا اور منظم رکھنا کافی مشکل کام ہے۔ اگر آپ اس کام کو با آسانی کرنا چاہیں تو ''ونڈوز اپ ڈیٹ منی ٹول'' (Windows Update MiniTool) استعمال کریں۔

اس ٹول کے ذریعے آپ چھ کام کرسکتے ہیں:

1- اپ ڈیٹ سرور سے رابطہ کرکے اپ ڈیٹس کی دستیابی چیک کریں

2- منتخب اپ ڈیٹس ڈاؤن لوڈ کریں لیکن انسٹال نہ کریں

3- منتخب اپ ڈیٹس ڈاؤن لوڈ اور انسٹال کریں

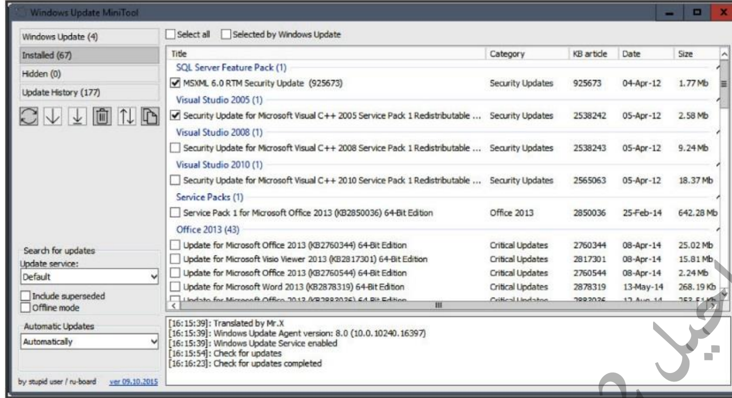
4- منتخب اپ ڈیٹس کو اَن انسٹال کریں

5- منتخب اپ ڈیٹس کو بلاک کریں

6- معلومات کو کلپ بورڈ پر کاپی کریں

یہ ٹول ہر اپ ڈیٹ کے بارے میں مائیکروسافٹ کی ویب سائٹ پر موجود معلوماتی مضمون کا لنک بھی ساتھ دِکھاتا ہے تاکہ آپ جان سکیں کہ یہ اپ ڈیٹ کس چیز سے متعلق ہے اور اس میں کیا موجود ہے۔

bit.ly/wum-tool



ونڈوز کا اپ ڈیٹ نہ ہونا ٹھیک کریں

''ری سیٹ ونڈوز اپ ڈیٹ ایجنٹ'' ایک چھوٹا سا کمانڈ کے ذریعے چلنے والا پروگرام ہے جو ونڈوز آپریٹنگ سسٹم کے اپ ڈیٹ نہ ہو پانے کی وجہ بننے والے مسائل کو حل کرتا ہے۔ ونڈوز اپ ڈیٹ ویسے تو مسائل کا شکار نہیں ہوتی لیکن کسی سروس کے نہ چل سکنے یا کسی اور صورت میں اپ ڈیٹس کو درست طریقے سے نہ ڈاؤن لوڈ یا انسٹال کر پا رہی ہو تو صارف کے لیے سمجھنا مشکل ہوجاتا ہے کہ اس کی وجہ کیا ہے۔

ونڈوز کی اپ ڈیٹس سے جُڑے مسائل حل کرنے کے لیے یہ چھوٹا سا ٹول بنایا گیا ہے۔ اس کے ہوتے ہوئے آپ پیچیدہ چیزیں دیکھنے سے بچ جاتے ہیں۔ اسے استعمال کرنے کے لیے ضروری ہے کہ آپ کے پاس ایڈمنسٹریٹر اختیارات موجود ہوں۔ اس لیے اس پر رائٹ کلک کرتے ہوئے ''رن ایز ایڈمنسٹریٹر'' کے ذریعے اسے چلائیں۔

جب آپ اسے چلائیں گے تو یہ دس آپشنز دکھائے گا۔ چونکہ عام طور پر کمپیوٹر صارفین کو نہیں پتا ہوتا کہ ونڈوز اپ ڈیٹ نہ ہو پا رہی ہو تو کیا کیا کرنا چاہیے اس لیے اس ٹول میں ونڈوز اپ ڈیٹ سے متعلقہ تمام آپشنز فہرست کی صورت میں موجود ہوں گے۔ چاہے ونڈوز رجسٹری ایڈیٹر میں کسی خرابی کی وجہ سے اپ ڈیٹ نہ ہو پا رہی ہو یا پہلے سے ڈاؤن لوڈ ادھوری اپ ڈیٹس کی وجہ سے، اس میں دیے گئے تمام آپشنز آپ باری باری آزما سکتے ہیں۔ جو آپشن منتخب کرنا ہو اس کا نمبر نیچے لکھ کر اینٹر پریس کردیں۔

صرف 29KB سائز کا حامل یہ ٹول ونڈوز اپ ڈیٹس سے متعلقہ تمام مسائل حل کرنے کی صلاحیت رکھتا ہے۔

bit.ly/reset-update



نوکیا لومیا فون کا سافٹ ویئر با آسانی ری انسٹال کریں

ویسے تو اینڈ رائیڈ فونز سب سے زیادہ مقبول ہیں کیونکہ اینڈ رائیڈ کے اوپن سورس ہونے کی وجہ سے اس کے سستے مہنگے ہر قسم کے فون دستیاب ہیں اور ہر کوئی اپنے بجٹ کے حساب سے فون خرید سکتا ہے۔ لیکن اینڈ رائیڈ کے علاوہ ونڈوز فون پسند کرنے والوں کی بھی ایک بڑی تعداد موجود ہے۔ نوکیا لومیا فونز کی آمد نے ونڈوز فون کی مقبولیت میں بے پناہ اضافہ کیا۔ اگر آپ کے پاس نوکیا لومیا فون موجود ہے اور اس کا آپریٹنگ سسٹم کچھ خرابی کے آثار دِکھا رہا ہے تو اس مسئلے کو ''ونڈوز ڈیوائس ریکوری ٹول'' کی مدد سے فیکٹری روم (ROM) امیج دوبارہ سے انسٹال کر کے ٹھیک کیا جا سکتا ہے۔

نوکیا فونز کے سافٹ ویئر سے متعلقہ مسائل کو حل کرنے کے لیے مائیکروسافٹ نے دو ٹولز فراہم کر رکھے ہیں۔ ونڈوز فون ورژن 8 پر چلنے والے



فونز کے لیے ''ونڈوز ڈیوائس ریکوری ٹول'' جبکہ دیگر تمام نوکیا فونز کے لیے ''نوکیا سافٹ ویئر ریکوری ٹول'' موجود ہے۔ اپنی ڈیوائس کے اعتبار سے آپ ان میں سے کسی ٹول کا انتخاب کر سکتے ہیں۔ ٹول کی انسٹالیشن کے بعد فون کو بذریعہ یو ایس بی کیبل پی سی سے جوڑیں۔

جیسے ہی ٹول فون کو پہچان لے آپ ''اپ ڈیٹنگ'' یا ''ری اسٹورنگ'' کسی ایک آپشن کا انتخاب کر سکتے ہیں۔ یہاں ایک بات یاد رکھیں کہ سافٹ ویئر کی اس ری انسٹالیشن میں فون پر موجود تمام ڈیٹا ختم ہو جائے گا اس لیے اس کام سے پہلے اپنے اہم ڈیٹا کو بیک اپ ضرور کر لیں۔

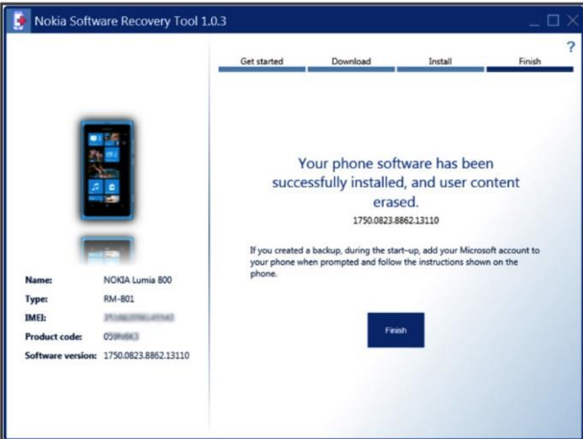
Continue کے بٹن پر کلک کریں تو یہ ٹول نوکیا کے سرور سے فون کے لیے روم امیج (ROM image) کا تازہ ترین ورژن ڈاؤن لوڈ کرنا شروع کر دے گا۔



روم مکمل ڈاؤن لوڈ ہونے پر فون میں انسٹال کر دی جائے گی لیکن اس میں کچھ وقت لگے گا اس لیے صبر سے انتظار کریں۔ انسٹالیشن کا یہ عمل جسے Flashing کہتے ہیں مکمل ہونے کے بعد فون کو ری اسٹارٹ کر دیا جائے گا۔ جس کے بعد آپ اسے استعمال کر سکتے ہیں۔

ونڈوز ڈیوائس ریکوری ٹول اور نوکیا سافٹ ویئر ریکوری ٹول ان پروگرامز کی مدد سے آپ خود با آسانی فون کا فرم ویئر ری سیٹ اور ری انسٹال کر سکتے ہیں۔ یہ دونوں ٹولز اور ان کو استعمال کرنے کا طریقہ مائیکروسافٹ کی ویب سائٹ پر ایک ہی صفحے پر موجود ہیں۔ یہاں دی گئی ہدایات کو ایک دفعہ ضرور پڑھیں اور اس کے بعد اپنے فون کے اعتبار سے ٹول ڈاؤن لوڈ کر کے استعمال کریں۔ یاد رہے چونکہ ٹول کو سافٹ ویئر مائیکروسافٹ کے سرور سے ڈاؤن لوڈ کرنا ہے اس لیے آپ کے پاس انٹرنیٹ کا چل رہا ہونا ضروری ہے۔

bit.ly/nokia-software-tool



ویب لنک دوست کے ویب براؤزر میں کھولیں۔ گوگل کروم

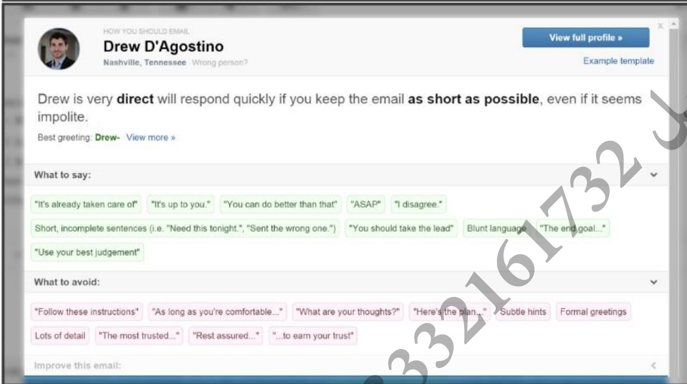


bit.ly/shove-chrome

ایک دوسرے کو ویب سائٹس کے مختلف لنکس بھیجنا ہمارا روزمرہ کا معمول ہے۔ اکثر ہم کسی کو کوئی لنک بھیجتے ہیں لیکن پتا نہیں چلتا کہ اس نے وہ لنک دیکھا یا نہیں۔ ایسا بھی ہوتا ہے کہ کمپیوٹر سے کم واقف لوگوں کو کوئی ویب سائٹ کھولنے کا کہیں اور وہ غلط ویب سائٹ کھول لیں۔ گوگل کروم کے لیے ایک نیا زبردست ایکسٹینشن ''شوو'' (Shove) سامنے آیا ہے۔

یہ ایکسٹینشن دونوں جگہ گوگل کروم براؤزر میں انسٹال ہونا چاہیے۔ اس کے علاوہ اس میں اکاؤنٹ بنا کر سائن اِن ہونا پڑتا ہے اور دوستوں کو ایڈ کرنا پڑتا ہے۔ اس کے بعد دوست ایک دوسرے کے براؤزر میں کوئی بھی کھول سکتے ہیں۔ یعنی لنک بھیجنا نہیں ہوگا بلکہ براہِ راست اگلے براؤزر میں کھل جائے گا۔

ای میل لکھنے کے فن میں مہارت حاصل کریں۔ گوگل کروم



پروفیشنل ای میل لکھنا کوئی آسان بات نہیں ہوتی۔ ای میل کس انداز میں لکھی جائے اس کا انحصار اس بات پر ہوتا ہے کہ ای میل کسے بھیجی جا رہی ہے۔ ظاہر ہے اپنے افسران سے اس انداز میں بات نہیں کی جاسکتی جیسے ہم کسی قریبی دوست سے کرتے ہیں۔ اگر آپ ای میل لکھنے کے فن میں مہارت حاصل کرنا چاہتے ہیں تو گوگل کروم میں ''کرسٹل'' ایکسٹینشن انسٹال کریں۔ یہ ایکسٹینشن پرسنیلٹی ڈٹیکشن ٹیکنالوجی سے لیس ہے، یعنی جسے ای میل بھیجی جا رہی ہو یہ اس کے بارے میں انٹرنیٹ پر گھوم کر چھان بین کر لیتا ہے۔ پھر ای میل لکھتے ہوئے آپ کو ایسے الفاظ فراہم کرتا ہے جنھیں استعمال کرکے آپ کی ای میل بن جاتی ہے شاندار۔

www.crystalknows.com

تصاویر پر لکھا متن با آسانی کاپی کریں۔ گوگل کروم

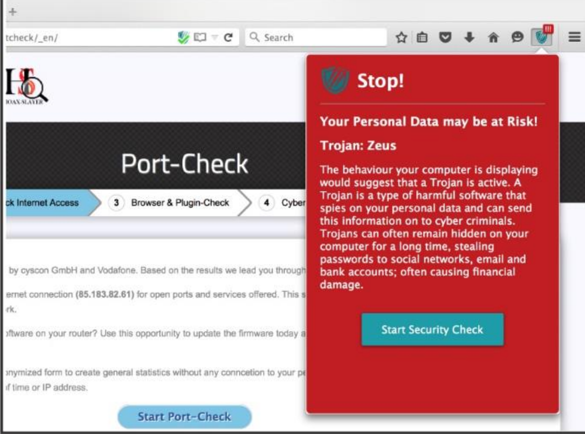


اکثر تصاویر پر لکھا ہوا متن (Text) ہمیں متاثر کرتا ہے اور ہم اسے اپنے پاس محفوظ کرنے کے لیے پوری تصویر ہی محفوظ کر لیتے ہیں۔ یقیناً کسی تصویر پر موجود ٹیکسٹ کاپی تو نہیں کیا جاسکتا، اس کام کے لیے کوئی او سی آر سافٹ ویئر درکار ہوگا۔ لیکن اب کسی سافٹ ویئر کی ضرورت نہیں کیونکہ گوگل کروم کے لیے ایک انتہائی شاندار اور دلچسپ ایکسٹینشن بنایا جاچکا ہے جو کسی بھی تصویر پر لکھا ہوا ٹیکسٹ کاپی کر سکتا ہے۔

اس ایکسٹینشن کا نام ''پروجیکٹ نیپتھا'' (Project Naptha) ہے۔ کروم میں اس کی انسٹالیشن کے بعد آپ کسی بھی تصویر پر رائٹ کلک کرتے ہوئے اس میں موجود ٹیکسٹ کو با آسانی کاپی کر سکتے ہیں۔

bit.ly/project-naptha

وائرس زدہ اور ہیک شدہ ویب سائٹس وزٹ کرنے سے بچیں۔ موزیلا فائرفوکس

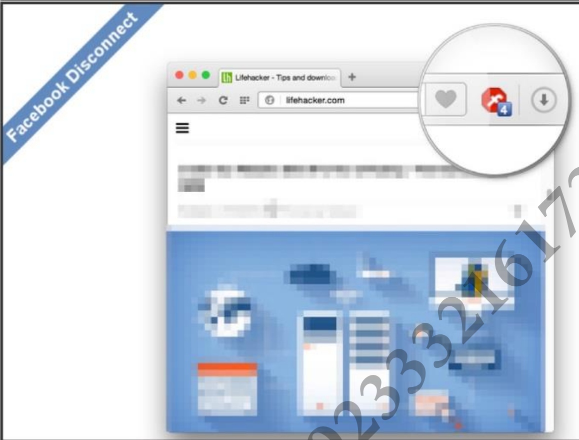


آئے دن کوئی نہ کوئی ویب سائٹ ہیک ہوتی رہتی ہے۔ عام صارف کو پتا ہی نہیں چلتا کہ وہ کسی وائرس زدہ ویب سائٹ پر ہے جو اسے نقصان بھی پہنچا سکتی ہے۔ یہی وجہ ہے کہ آن لائن محفوظ رہنا کافی مشکل ہو چکا ہے۔ آن لائن کسی نقصان سے بچنے کے لیے آپ اپنے فائرفوکس براؤزر میں cyscon Security Shield انسٹال کر سکتے ہیں۔ جب بھی آپ کسی وائرس زدہ یا ہیک شدہ ویب سائٹ پر جائیں گے یہ ایکسٹینشن فوراً آپ کو مطلع کرے گا۔

اپنی پرائیویسی اور ذاتی ڈیٹا کی حفاظت کے لیے اس ایکسٹینشن کو آپ سکیورٹی کی ایک اضافی تہہ کے طور پر استعمال کر سکتے ہیں۔

bit.ly/cyscon-security

ویب سائٹس کو فیس بک کے ذریعے اپنی جاسوسی سے باز رکھیں۔ موزیلا فائرفوکس

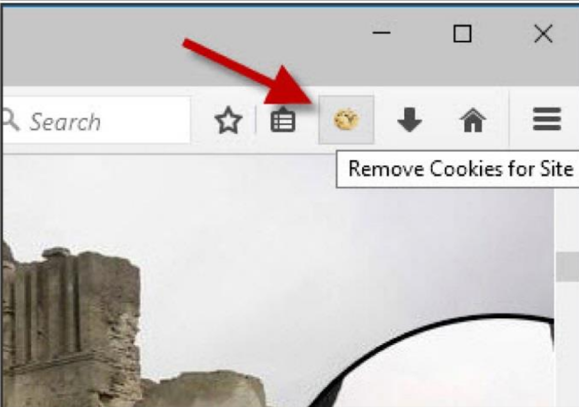


فیس بک کی ایک بڑی خرابی یہ ہے کہ جب آپ اسے استعمال نہیں کر رہے ہوتے تب بھی اس کے ذریعے آپ کی جاسوسی کی جا رہی ہوتی ہے۔ اس جاسوسی کے ذریعے آپ کی دلچسپی اور ضروریات کو جاننے کے بعد اسی حوالے سے اشتہارات دِکھائے جاتے ہیں۔ اگر آپ ویب سائٹس کی اپنی ذاتی زندگی میں اس تانک جھانک کو بند کرنا چاہتے ہیں تو اپنے موزیلا فائرفوکس براؤزر میں "فیس بک ڈسکنیکٹ" ایکسٹینشن انسٹال کریں۔

یہ ایکسٹینشن ویب سائٹس کی آپ کے فیس بک اکاؤنٹ سے جُڑنے کی تمام کوششوں کو بلاک کر دیتا ہے۔ حتیٰ کہ نمبر بھی بتاتا ہے کہ کتنے ٹریکر بلاک کیے گئے۔

bit.ly/fb-disconnect

کسی ویب سائٹ کی تمام کوکیز حذف کریں۔ موزیلا فائرفوکس



آپ جب کوئی ویب سائٹ دیکھتے ہیں تو ویب سائٹ آپ کے کمپیوٹر میں چھوٹی چھوٹی فائلز بناتی ہے جنھیں کوکیز کہتے ہیں۔ آپ نے ویب سائٹ پر کیا سرگرمیاں انجام دیں اس حوالے سے معلومات کوکیز میں محفوظ ہوتی ہے۔ مثلاً آپ نے آخری دفعہ اس ویب سائٹ کو کب دیکھا تھا اور کس کس صفحے پر گئے تھے وغیرہ۔

کسی بھی ویب سائٹ کی تمام کوکیز کمپیوٹر سے صاف کرنے کا آپشن ویسے تو براؤزر میں موجود ہوتا ہے لیکن اس کام کو مزید آسان بنانے کے لیے "ریموو کوکیز" ایکسٹینشن فائرفوکس میں انسٹال کر کے کسی بھی ویب سائٹ کی تمام کوکیز کو صرف ایک کلک سے حذف کیا جا سکتا ہے۔ bit.ly/remove-cookies



اینڈرائیڈ کے لئے شاندار "بیٹری بچاؤ" ایپلی کیشنز

امر کمار

ایک وقت ہوا کرتا تھا کہ فون صرف بات کرنے کے لیے کام آتے تھے۔ اگر آپ نے نوکیا کے پرانے موبائل استعمال کیے ہیں تو آپ کو پتا ہوگا کہ وہ فون ایک بار فل چارج کرنے پر دو تین دن آرام سے نکال لیتے تھے۔ آج کل کے موبائل بہت ہی تیز ہو گئے ہیں اور ایک پینٹیم 3 کمپیوٹر جتنا کام کر سکتے ہیں۔ کچھ فون تو اس سے بھی بہتر ہیں۔ اب ہم فون پر صرف بات ہی نہیں کرتے بلکہ میسج کرتے ہیں، ای میل کرتے ہیں، فیس بک چلاتے ہیں اور بہت سارے کام کرتے ہیں۔ لیکن اتنے سارے نئے فیچرز کے ساتھ ایک مسئلہ ہے اور وہ ہے فون کی بیٹری۔ فون کی بیٹری اگر اب ایک دن بھی نکال لے تو بڑی بات ہے۔

لیکن اینڈرائیڈ پر بہت سی ایسی ایپلی کیشنز ہیں جو آپ کے فون کی بیٹری کو کچھ دیر زیادہ چلا سکتی ہیں۔ ان میں سے کچھ بہترین ایپلی کیشنز ہم نے آپ کے لیے منتخب کی ہیں۔ آیئے ان کا تفصیلی جائزہ لیتے ہیں تا کہ آپ اپنی ضرورت اور پسند کے تحت کسی ایپلی کیشن کو منتخب کر سکیں۔

1: بیٹری ڈاکٹر (Battery Doctor)

بیٹری ڈاکٹر ایک ایسی بیٹری سیونگ ایپ ہے جسے تقریباً سب جانتے ہیں اور اسے کبھی نہ کبھی استعمال بھی کیا ہوگا۔ اس کا دعویٰ ہے کہ یہ آپ کے فون کی بیٹری ٹائمنگ ڈبل کر دیتی ہے اور یہ کچھ حد تک صحیح بھی ہے۔

اس میں آپ ایک ہی کلک سے ان تمام ایپس کو بند کر سکتے ہیں جو بیٹری ختم کر رہی ہوتی ہیں۔ اس کے ساتھ ساتھ ایک اور شاندار فیچر یہ ہے کہ یہ آپ کے فون کو تھوڑا سا جلدی بھی چارج کرتا ہے۔

بیٹری ڈاکٹر کی مدد سے آپ کا فون پہلے سے کم از کم 20 منٹ جلدی چارج ہوتا ہے۔ بیٹری ڈاکٹر کی مدد سے آپ یہ بھی جان سکیں گے کہ کون سی ایپ سب سے زیادہ بیٹری استعمال کر رہی ہے اور کتنی دیر تک فون اس بیٹری پر آن رہ سکتا ہے۔





اس کے علاوہ یہ بیٹری کی حالت اور اس کا درجہ حرارت (temperature) بھی بتاتی ہے۔ اس کے علاوہ اس میں بہت ہی اعلیٰ قسم کے بیٹری سیونگ موڈز ہیں جو بیٹری کا زیادہ دیر چلنا ممکن بناتے ہیں۔

گوگل پلے اسٹور سے انسٹال کرنے کے لیے درج ذیل ربط ملاحظہ کریں:

bit.ly/battery-doc-app

2: ڈی یو بیٹری سیور (DU Battery Saver)





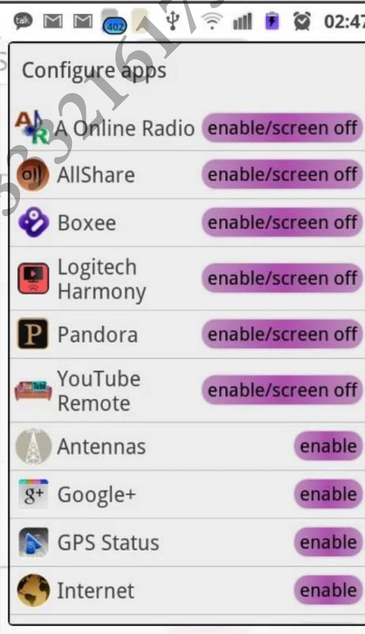
ڈی یو بیٹری سیور سب سے زیادہ ڈاؤن لوڈ کیا گیا بیٹری سیور ہے۔ اس میں ایک کلک سے بیٹری کو آپٹیمائز کیا جاسکتا ہے۔ اس کے علاوہ اس میں آپ اپنی پسند کی پروفائل بھی بنا سکتے ہیں۔ مثلاً اگر آپ دوپہر کو وائی فائی استعمال نہیں کرتے تو 1 بجے سے 4 بجے تک کی ایک پروفائل بنائیں جس میں وائی فائی آف کردیں تو اس وقت کے دوران وائی فائی خودبخود بند ہوجائے گا۔

اس کے علاوہ آپ رات کے وقت اگر کال اٹینڈ نہیں کرتے تو پروفائل میں ایئرپلین موڈ آن کردیں۔ اس کے علاوہ یہ ایک دلکش انٹرفیس کی مالک بھی ہے۔ اس میں ایک چارج منیجر کا فیچر ہے جو آپ کی بیٹری کا خیال رکھتا ہے اور آپ کو بتاتا ہے کہ کون سے دن آپ نے اپنے فون کو کتنی دیر چارج کیا تھا۔

گوگل پلے اسٹور سے انسٹال کرنے کے لیے درج ذیل ربط ملاحظہ کریں: bit.ly/du-battery-saver

3: جوس ڈیفینڈر (JuiceDefender)





جوس ڈیفینڈر اصل میں تین ورژن میں آتا ہے۔ ایک ورژن فری ہے اور باقی دو پیسوں سے خریدے جاتے ہیں۔ لیکن آپ کو پیسوں سے خریدنے کی ضرورت نہیں کیونکہ اس کا مفت والا ورژن بھی کمال ہے۔ اس میں بیٹری سیونگ کے تین موڈ ہیں۔ پہلا ہے متوازن (balanced) جو ایک عام موڈ ہے اور اس سے آپ فون کی بیٹری ٹائمنگ تقریباً 4-6 گھنٹوں تک بڑھ جاتی ہے۔

دوسرا موڈ غصیلا یعنی aggressive ہے اور تیسرا انتہائی یعنی extreme ہے۔ ایکسٹریم موڈ آن کرکے آپ ڈگنی ٹائمنگ حاصل کرسکتے ہیں۔

اس کے علاوہ اس میں آپ کسٹمائزڈ موڈ مطلب اپنی ضرورت کے حساب سے بھی موڈ بنا سکتے ہیں۔ اس کا ایک اور شاندار فیچر وائی فائی کا وقت کے حساب سے آن یا آف ہونا ہے۔ اگر آپ چاہتے ہیں کے آپ فون کی ایپلی کیشنز شام کے وقت اپ ڈیٹ ہوجائیں تو آپ وائی فائی کے آن ہونے کا ٹائم سیٹ کردیجیے۔

گوگل پلے اسٹور سے انسٹال کرنے کے لیے درج ذیل ربط ملاحظہ کریں:

bit.ly/juice-defender

ورڈ پریس کے nulled تھیم کیا استعمال کرنے چاہئے؟

تحریر: امانت علی گوہر

ورڈ پریس (WordPress) اس وقت دنیا کا مقبول ترین اور سب سے زیادہ پسند کیا جانے والا کانٹینٹ منیجمنٹ سسٹم (CMS) ہے۔ انٹرنیٹ پر موجود کروڑوں ویب سائٹس ورڈ پریس پر مبنی ہیں۔ وکی پیڈیا کے مطابق انٹرنیٹ پر مقبول پہلی ایک کروڑ ویب سائٹس میں سے 23.3 فیصد ویب سائٹس ورڈ پریس استعمال کر رہی ہیں۔ ورڈ پریس کا سب سے پسندیدہ فیچر تھیم اور پلگ اِنز ہیں۔ ورڈ پریس کے ہزاروں یا شاید لاکھوں تھیم دستیاب ہیں جن کے ذریعے منٹوں میں کسی ویب سائٹ کا مکمل حلیہ تبدیل کیا جا سکتا ہے۔ کچھ تھیم قیمتاً دستیاب ہوتے ہیں اور کچھ مفت دستیاب ہوتے ہیں۔ قیمتاً دستیاب تھیم زیادہ قابل دید ہوتے ہیں اور پسند کئے جاتے ہیں۔ جیسا کہ ہر قیمتاً دستیاب سافٹ ویئر کے ساتھ پائیریسی کا مسئلہ چولی دامن کی طرح ساتھ رہتا ہے، اسی طرح قیمتاً دستیاب ورڈ پریس تھیم جنہیں پریمیئم تھیم کہا جاتا ہے، بھی کریک (crack) حالت میں انٹرنیٹ پر بہ آسانی مل جاتے ہیں۔ ہمارے یہاں بدقسمتی سے ورڈ پریس تھیم کے لئے لائسنس خریدنے کا رواج پروان نہیں چڑھ سکا۔ خاص طور پر اپنی ذاتی ویب سائٹ کے لئے لوگ خرچہ کرنے کے بجائے غیر قانونی طریقے سے حاصل کئے گئے تھیم جنہیں nulled تھیم بھی کہا جاتا ہے، استعمال کرتے ہیں۔ حالانکہ تھیم کی قیمت ایک ہزار روپے سے لیکر پانچ ہزار تک ہوتی ہے۔ اگر کوئی شخص کئی ہزار روپے کا کمپیوٹر خرید سکتا ہے، یا ویب ہوسٹنگ کے لئے ہزاروں روپے خرچ کر سکتا ہے تو اس کے لئے تھیم خریدنا کیونکر مشکل ہوگا؟ لیکن بدقسمتی سے دنیا بھر میں nulled تھیم بڑے پیمانے پر استعمال کئے جاتے ہیں جو بعد میں شدید نقصان کا باعث بھی بن جاتے ہیں۔

جس طرح کریک سافٹ ویئر کو استعمال کرنا خطرے سے خالی نہیں، اسی طرح nulled تھیم کا استعمال بھی گلے پڑ سکتا ہے۔ یہ تھیم ہیکروں کا سب سے بہترین ہتھیار ہے جس کے ذریعے وہ ویب سائٹس کو ہیک کرتے ہیں یا ویب سائٹ ملاحظہ کرنے والوں کو نقصان پہنچانے کی کوشش کرتے ہیں۔ ہیکر پریمیئم تھیم خرید کر یا چوری کر کے انٹرنیٹ پر تو مفت آن لائن کر دیتے ہیں، لیکن ساتھ ہی اس میں مال ویئر، ہیکنگ اسکرپٹ یا بیک ڈور بھی شامل کر دیتے ہیں۔ بیشتر ہیکنگ اسکرپٹ اس طرح سے تیار اور تھیم کا حصہ بنائے جاتے ہیں کہ اینٹی وائرس بھی ان کو پہچان نہیں پاتا۔

جب یہی متاثرہ تھیم کوئی ڈاؤن لوڈ کر کے اپنی ویب سائٹ پر استعمال کرتا ہے تو ویب سائٹ اگلے ہی لمحے یا کسی خاص موقع پر infected ہو جاتی ہے۔ انفیکشن کے بعد ویب سائٹ کا حلیہ بگڑ سکتا ہے یا بیشتر موقع پر ویب سائٹ کے ناظرین کو کسی دوسری بے ہودہ یا دھوکہ دہی پر مبنی ویب سائٹ کی جانب موڑ دیا جاتا ہے۔ گوگل کو جیسے ہی محسوس ہوتا ہے کہ ویب سائٹ infected ہے، وہ فوراً تلاش کے نتائج میں ویب سائٹ کے روابط کے نیچے ایک انتباہ بھی دینا شروع کر دیتا ہے کہ یہ ویب سائٹ شاید آپ کے کمپیوٹر کو نقصان پہنچا سکتی ہے۔ اگر آپ کی ویب سائٹ پر کمائی کے لئے اشتہارات چلتے ہیں تو انفیکشن کی صورت میں ان اشتہارات سے بھی آپ کو ہاتھ دھونا پڑ سکتا ہے۔ انفیکشن کے بعد ویب سائٹ پر آنے والا ٹریفک شدید متاثر ہوتا ہے۔

کچھ مال ویئر اور ہیکنگ اسکرپٹ اس قدر خطرناک ہوتے ہیں کہ وہ سرور کی خامیوں کا فائدہ اٹھا کر اس کا ستیاناس کر دیتے ہیں۔ ایک کیس میں ہم نے یہ بھی دیکھا کہ nulled اسکرپٹ کے استعمال کی وجہ سے لینکس سرور پر موجود تمام ڈیٹا فائلیں ransomware سے متاثر ہو گئیں اور ایڈمنسٹریٹر کو بھاری مالی نقصان جو تھیم کی قیمت سے سینکڑوں گنا تک زیادہ تھا، برداشت کرنا پڑا۔

کریک تھیم استعمال کرنے والے اس تھیم کی اپ ڈیٹس سے بھی محروم رہتے ہیں۔ ورڈ پریس میں بہتری پیدا کرنے یا سکیورٹی خامیاں دور کرنے کے لئے اس کی اپ ڈیٹس تواتر سے جاری کی جاتی ہیں۔ ان اپ ڈیٹس کی وجہ سے تھیم کو بھی نئی تبدیلیوں کے ساتھ ہم آہنگ کرنے کے لئے اپ ڈیٹ کیا جاتا ہے۔ لہٰذا اگر تھیم کو اپ ڈیٹ نہ کیا جائے لیکن ورڈ پریس کو اپ ڈیٹ کر دیا جائے یا پلگ ان اپ ڈیٹ کر دیئے جائیں تو ویب سائٹ کا حلیہ یا کام کرنے کا انداز بالکل تبدیل ہو سکتا ہے۔

اگر nulled تھیم کی وجہ سے آپ کی ویب سائٹ مال ویئر سے متاثر ہو جاتی ہے تو بیشتر ہوسٹنگ پرووائیڈر کمپنیاں آپ کا ہوسٹنگ اکاؤنٹ ہی منسوخ کر دیتی ہیں۔ نیز، آپ کی ویب سائٹ پر وائرس سے متاثرہ ہونے کا دھبہ انٹرنیٹ پر ہمیشہ کے لئے قائم ہو جاتا ہے۔ اس لئے nulled تھیم کا استعمال عارضی طور پر چند ہزار روپے تو بچا سکتا ہے، لیکن مستقبل میں ہزاروں یا شاید لاکھوں کے نقصان کا باعث بھی بن سکتا ہے۔



درج ذیل آسان سوالوں کے جوابات دے کر آپ حاصل کرسکتے ہیں، **2000** روپے تک کا کیش پرائز

1) SSL کن الفاظ کا مخفف ہے؟

☆سیکیور سائٹ لیئر ☆سائٹ سکیورٹی لیئر ☆سیکیور ساکٹس لیئر

2) کمپیوٹر نیٹ ورکنگ کے OSI Model میں کتنی layers ہوتی ہیں؟

☆تین ☆چار ☆سات

3) A+ سرٹیفکیشن کا امتحان کون سا ادارہ لیتا ہے؟

☆مائیکروسافٹ ☆CompTIA ☆اوریکل

☆......ان سوالات کے جوابات 30 نومبر تک ارسال کئے جاسکتے ہیں۔

☆......کوپن پر جوابات لکھ کر اس کوپن کی اسکین کاپی یا موبائل سے فوٹو کھینچ کر بھی بھیجا جاسکتا ہے۔

☆......موصول ہونے والے ای میل پیغامات چونکہ بہت زیادہ ہوتی ہیں، اس لئے کوپن مل جانے کی اطلاع دینا ہمارے لئے ممکن نہیں۔

پہلا انعام 2000 روپے نقد	(ایک انعام)
دوسرا انعام 200 روپے نقد	(10 انعامات)

ماہ اگست کے سوالات کے درست جوابات

❶ پانچویں نسل ❷ انٹرنیٹ میل ایکسچینج پروٹوکول

❸ ایپل

پہلا انعام

فہیم الدین، کراچی

دوسرا انعام جیتنے والے دس قارئین

☆ اذان خان، کراچی ☆ محمد مشتاق، کراچی ☆ محمد اقبال، کراچی ☆ فہمیدہ، لاہور ☆ جمال عبدالناصر، کراچی ☆شکیل احمد، سرگودھا ☆ کامران، کراچی ☆ علی جعفری، کراچی ☆ جہانزیب قادری، لاہور ☆علی احمد، سانگھڑ

انعامی کوپن برائے نومبر 2015ء

جوابات: 1)............ 2)............ 3)............

نام............ فون نمبر............

پتا............

....

یہ کوپن crm@computingpk.com پر ای میل کیجئے یا ''ماہنامہ کمپیوٹنگ''، پوسٹ باکس نمبر 786، کراچی 74200 پر بذریعہ ڈاک ارسال کیجئے

کوالکوم سرورز کی تیاری میں مگن

کوالکوم کو لوگ اسمارٹ فون کے لئے پروسیسر بنانے کے حوالے سے جانتے ہیں ۔ ان کے اسنیپ ڈریگن چپ سیٹ کئی مہنگے اور اعلیٰ کارکردگی کے حامل اسمارٹ فونز اور ٹیبلیٹس میں استعمال کئے جاتے ہیں۔ لیکن اب کوالکوم صرف اسمارٹ فونز اور ٹیبلیٹس تک محدود نہیں رہنا چاہتا۔ بلکہ اس کا ارادہ ہارڈویئر کی ایک بڑی کمپنی سے براہ راست ٹکر لینے کا ہے۔ جی ہاں، کوالکوم چاہتا ہے کہ وہ اے آر ایم پروسیسرز پر مبنی سرورز تیار کرے۔

اس حوالے سے ابتدائی خبریں ایک سال پہلے آئی تھیں۔ لیکن اس کے بعد کوالکوم کی جانب سے خاموشی چھائی رہی اور یہ واضح نہیں ہوسکا کہ آخر کمپنی اس میدان میں کیا تیر مارنا چاہتی ہے۔ تقریباً چھ ماہ پہلے کمپنی نے چپ سیٹس تیار کرنے والی چینی کمپنی AllWinner کے ساتھ شراکت داری قائم کی تھی تاکہ سستے LTE ٹیبلیٹس تیار کئے جاسکیں۔ جبکہ دوسری جانب کمپنی ARM کے ساتھ مل کر ایک 64 کورز پر مبنی پروسیسر پر بھی کام کررہی ہے۔

اب جا کر کوالکوم کے سرورز کے بارے میں مزید خبریں سامنے آئی ہیں، جن سے اندازہ ہوتا ہے کہ کوالکوم کیوں اتنے عرصے سے خاموش تھا۔

سرورز کی مارکیٹ کوئی چھوٹی مارکیٹ نہیں ہے۔ اس مارکیٹ پر انٹل کی اجارہ داری ہے جو بعض اوقات اپنے سرور پروسیسرز کے لئے پاگل پن کی حد تک زیادہ رقم طلب کرتا ہے۔ مثلاً یکم جون 2015ء کو جاری کئے جانے والی انٹل زیون پروسیسر E5-4669 جو کہ 18 کورز پر مبنی ہے، کی ابتدائی قیمت تقریباً سات لاکھ پاکستانی روپوں کے لگ بھگ تھی۔ کچھ ایسی ہی صورت حال اے ایم ڈی کے سرور پروسیسرز کے ساتھ بھی درپیش ہے۔ نہلے پر دہلا کہ ان کمپنیوں کے سرور پروسیسر بہت زیادہ توانائی خرچ ہوتے ہیں۔ جس زیون پروسیسر کا ہم نے اوپر ذکر کیا ہے، اس کا ٹی ڈی پی (تھرمل ڈیزائن پاور) 145 واٹ ہے۔ یہی وجہ ہے کہ سستے اور کم توانائی خرچ سرورز کی ضرورت ہمیشہ سے رہی ہے۔ اس حوالے سے اے آر ایم پروسیسر پر مبنی سرورز ایک بہترین متبادل ثابت ہوسکتے ہیں اور کچھ کمپنیاں پہلے ہی ایسے سرور فروخت کررہی ہیں جن میں اے آر ایم پروسیسر استعمال کئے گئے ہیں۔

کوالکوم سرور کی مارکیٹ میں داخلے کے لئے بے حد سنجیدہ ہے اسی لئے یہ مارکیٹ میں ایک توپ چیز لے کر آیا ہے۔ یہ چیز کوالکوم کا نیا اے آر ایم آرکیٹکچر پر مبنی 24 کور (vigintiquattuor-core) پروسیسر ہے۔ کوالکوم کا یہ 24 کور پروسیسر ورژن ابھی صرف ایک پروٹو ٹائپ ہے۔ حتمی ورژن میں زیادہ کور ہونگے۔ یہ بنیادی طور پر ایک سسٹم آن چپ ہے جس پر PCIe اور اسٹوریج کنٹرولر بھی موجود ہیں۔ یہ 24 کور پروسیسر دراصل 64 کور کے پروسیسر، جسے ہائیڈرا (Hydra) کا کوڈ نیم دیا گیا ہے، کی جانب ایک قدم ہے۔

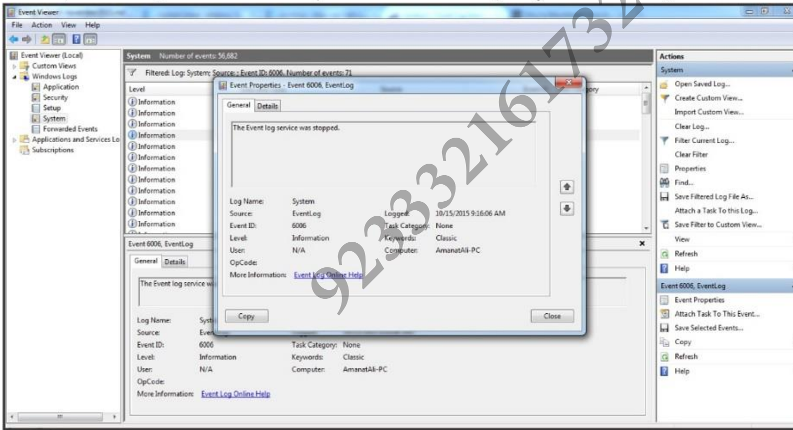
64 کورز ہونے کے باوجود اے آر ایم پروسیسرز کا مقابلہ زیون سرورز کے ساتھ نہیں کیا جاسکتا۔ اے آر ایم پروسیسرز پر مبنی سرورز بنانے کا مقصد سستے اور کم توانائی خرچ سرورز بنانا ہے۔ لیکن اس میں ایک قباعت یہ بھی ہے کہ تقریباً تمام ہی آپریٹنگ سسٹم اور ایپلی کیشنز x86 یا x64 آرکیٹکچر کے لئے بنائی جاتی ہیں اور یہ اے آر ایم سرورز پر نہیں چل سکتیں۔ اس لئے اے آر ایم سرورز کا استعمال مستقبل قریب تک محدود پیمانے پر ہی کیا جاتا رہے گا اور اس سے انٹل اور اے ایم ڈی کی اجارہ داری پر کوئی کاری ضرب نہیں لگے گی۔

پی سی DOCTOR

پی سی ڈاکٹر کے لئے اپنے سوالات editors@computingpk.com پر ارسال کیجئے یا ہمارے فیس بک فین پیج پر بذریعہ ذاتی پیغام ارسال کیجئے۔
کسی پوسٹ پر تبصرے کی صورت میں کئے گئے سوالات پر توجہ نہیں دی جاتی۔ کمپیوٹنگ میں صرف چند منتخب سوالات اور ان کے جوابات ہی شائع کئے جاتے ہیں

سوال: کیا ایسا کوئی طریقہ ہے جس کے ذریعے میں جان سکوں کہ آیا میری غیر موجودگی میں کسی نے میرا لیپ ٹاپ یا کمپیوٹر چلایا تھا کہ نہیں۔ اور اگر یہ بھی پتا چل سکے کہ کتنی دیر تک چلایا تھا تو بہت اچھا ہوگا۔ (فہیم خان، ای میل)

جواب: جی ہاں، بغیر کسی تھرڈ پارٹی سافٹ ویئر کے اس بات کا پتا چلایا جاسکتا ہے کہ آپ کی غیر موجودگی میں کسی نے لیپ ٹاپ یا کمپیوٹر آن/اسٹارٹ کیا تھا یا نہیں۔ نیز، یہ بھی پتا لگایا جاسکتا ہے کہ اسے کتنی دیر تک استعمال میں رکھا گیا۔ سب سے آسان طریقہ تو یہ ہے کہ آپ انٹرنیٹ ایکسپلورر یا کمپیوٹر میں نصب کسی دوسرے ویب براؤزر کو کھول کر اس کی ہسٹری چیک کریں۔ اگر آپ کی غیر موجودگی میں کمپیوٹر پر انٹرنیٹ استعمال کیا گیا ہے تو ہسٹری میں کچھ معلومات موجود ہوسکتی ہے۔ لیکن یہ طریقہ صرف اسی وقت کارگر ہے جب کمپیوٹر کے ساتھ انٹرنیٹ بھی استعمال کیا گیا ہو اور استعمال کرنے والا اتنا شاطر نہ ہو کہ اس نے ہسٹری صاف کردی ہو۔ تھوڑا پیچیدہ لیکن کافی حد تک کارگر طریقہ Event Viewer کی جانچ ہے۔ کنٹرول پینل میں Administrative Tools پر ڈبل کلک کریں اور وہاں موجود Event Viewer کے آئی کن پر ڈبل کلک کریں۔ آپ کے کمپیوٹر یا لیپ ٹاپ میں ہونے والی ہر اہم سرگرمی جس کا تعلق آپریٹنگ سسٹم یا کمپیوٹر

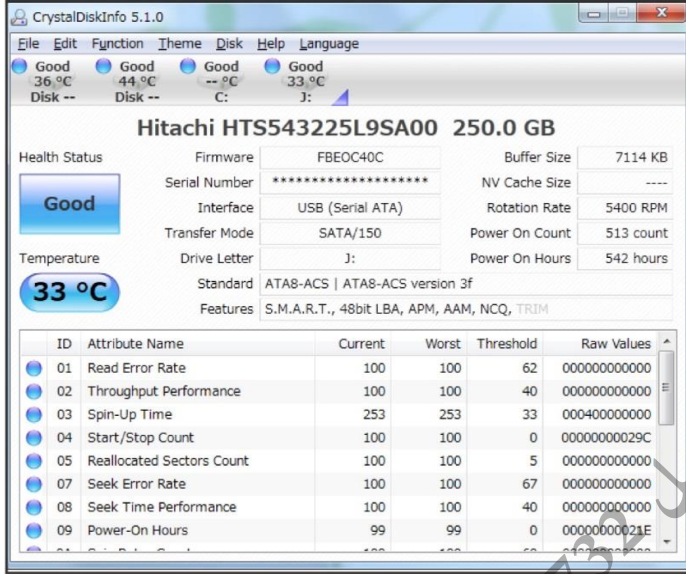


ہارڈ ویئر سے ہے، مائیکروسافٹ ونڈوز اس کا ریکارڈ رکھتی ہے۔ یہ ریکارڈ ایونٹ ویور کے ذریعے ملاحظہ کیا جاسکتا ہے۔ ایونٹ ویور میں بائیں جانب موجود فہرست میں سے Windows Logs کے تحت موجود System پر کلک کریں۔ دائیں جانب واقعات یا ایونٹس کی ایک طویل فہرست ظاہر ہوجائے گی۔ کمپیوٹر یا لیپ ٹاپ جب بوٹ کیا جاتا ہے تو ونڈوز کی درجنوں سروسز بھی چلتی ہیں۔ ان میں سے ایک سروس Event Viewer کی بھی ہے۔ ہم اگر یہ پتا لگالیں کہ ایونٹ ویور کی سروس کب چلی، ہم یہ بتا سکتے ہیں کہ کمپیوٹر کب چلایا گیا۔ لہٰذا ایونٹ ویور میں دائیں جانب Actions میں موجود Filter Current Log پر کلک کریں۔ جونہی ونڈو کھلے، اس میں All Event IDs کی جگہ پر 6005 لکھیں اور OK کے بٹن پر کلک کردیں۔ ایونٹ ویور میں اب صرف ایسے ایونٹ ظاہر ہونگے جن کی آئی ڈی 6005 ہے۔ یہ آئی ڈی دراصل Event Viewer کی سروس اسٹارٹ ہونے سے متعلق ہے۔ اب آپ یہ غور کیجئے کہ کیا آپ کی غیر موجودگی کے وقت کوئی ایونٹ بنا؟ اگر ہاں، تو جس وقت یہ ایونٹ بنا، وہ وقت نوٹ کرلیں کیونکہ یہی وہ وقت ہے جب کمپیوٹر کو بوٹ کیا گیا۔

اب دوبارہ Filter Current Log پر کلک کریں اور اب کی بار ایونٹ آئی ڈی میں 6006 لکھیں۔ یہ ایونٹ آئی ڈی ایونٹ سروس کے شٹ ڈاؤن یا بند ہونے سے متعلق ہے۔ یہ سروس اس وقت شٹ ڈاؤن ہوتی ہے جب کمپیوٹر کو شٹ ڈاؤن کیا جاتا ہے۔ فلٹر لگانے کے بعد جو ایونٹس آپ کو دِکھائی دیں، ان میں سے آپ اپنی غیر موجودگی میں پیش آنے والا ایونٹ تلاش کریں۔ یوں آپ بہ آسانی پتا چلاسکتے ہیں کہ کمپیوٹر کو کب چلایا گیا اور کب بند کیا گیا۔

سوال: میرے پاس ایک پرانی ہارڈ ڈرائیو ہے جس میں کافی قیمتی ڈیٹا محفوظ ہے۔ یہ ہارڈ ڈرائیو اِس وقت بالکل صحیح کام کر رہی ہے لیکن چونکہ یہ کافی پرانی ہے اس لئے مجھے خدشہ ہے کہ یہ کہیں خراب نہ ہو جائے۔ کیا ایسا کوئی طریقہ ہے جس سے معلوم کیا جاسکے کہ ہمارے زیر استعمال ہارڈ ڈرائیو کہیں خراب تو ہونے والی نہیں ہے۔ (فیصل، فیس بک)

جواب: ہارڈ ڈرائیو کب خراب ہو جائے، یہ بتانا ممکن نہیں۔ کچھ ہارڈ ڈرائیو چند ماہ بھی نہیں چل پاتیں اور کچھ سالوں تک بغیر کسی پریشانی کے کام کرتی رہتی ہیں۔ ہارڈ ڈرائیو کسی ایک مخصوص وجہ سے خراب نہیں ہوتی بلکہ اس کی سینکڑوں وجوہ ہوسکتی ہیں۔ ہوسکتا ہے کہ سو فی صد صحت مند ہارڈ ڈرائیو اگلے ہی لمحے کسی بیرونی عمل مثلاً بجلی کی کمی بیشی کی وجہ سے جواب دے جائے۔ اسی طرح یہ بھی عین ممکن ہے کہ کسی ہارڈ ڈرائیو کی موٹر چلتے چلتے اچانک ڈسک سے ٹکرا جائے۔ جبکہ ہارڈ ڈرائیو کے اونچائی سے گر کر خراب ہونے کا خدشہ تو ہمیشہ رہتا ہے۔ یہ ایسے عوامل ہیں جن کی پیش گوئی کرنا ناممکن کام ہے۔ البتہ ہارڈ ڈرائیو میں وقت کے ساتھ ساتھ کچھ طبعی اور کچھ لاجیکل تبدیلیاں واقع ہوتی ہیں جو بعد میں ہارڈ ڈرائیو کی مکمل موت کا باعث ہوسکتی ہیں۔ ان تبدیلیوں یا خرابیوں کا پتا لگا کر کسی ہارڈ ڈرائیو کے بارے میں پیشگی طور پر اندازہ لگایا جاسکتا ہے کہ وہ کس حد تک قابل بھروسہ ہے۔



ہارڈ ڈرائیو میں ایک نظام S.M.A.R.T (سیلف مونیٹرنگ اینالیسس اینڈ رپورٹنگ ٹیکنالوجی) بھی موجود ہوتا ہے۔ یہ نظام ہارڈ ڈرائیو میں پیدا ہونے والی خرابیوں پر نظر رکھتا ہے اور ان کے بارے میں مطلع کرتا ہے۔ اس نظام کی بدولت یہ بتانا ممکن ہے کہ آیا ہارڈ ڈرائیو کا وقت انتقال قریب تو نہیں آرہا۔ اگر S.M.A.R.T کو محسوس ہو کہ ہارڈ ڈرائیو میں کوئی خرابی پیدا ہوگئی ہے یا پیدا ہو رہی ہے تو وہ اس حوالے سے صارف تک اطلاع پہنچانے کی کوشش کرتا ہے۔ یہ اطلاع کمپیوٹر کے اسٹارٹ ہوتے ہی نظر آسکتی ہے یا پھر بایوس میں دیکھی جاسکتی ہے۔ ہمارے ہاں زیادہ تر مائیکروسافٹ ونڈوز استعمال کی جاتی ہے لیکن بدقسمتی سے ونڈوز میں ایسا کوئی ٹول موجود نہیں جو کمپیوٹر میں نصب ہارڈ ڈرائیو کے S.M.A.R.T ڈیٹا کو دیکھنے کے لئے استعمال کیا جاسکے۔ اس لئے تھرڈ پارٹی سافٹ ویئر استعمال کرنے پڑتے ہیں۔ خوش قسمتی سے اس مقصد کے لئے درجنوں مفت سافٹ ویئر دستیاب ہیں۔ تاہم مائیکروسافٹ ونڈوز میں ہارڈ ڈرائیو کی حالت (اسٹیٹس) چیک کرنے کے لئے کچھ کمانڈز موجود ہیں۔ کمانڈ پرامپٹ کھول کر اس میں wmic ٹائپ کر کے اینٹر کا بٹن دبائیں۔ اس کے بعد diskdrive get status لکھ کر اینٹر کریں۔ اگر ڈرائیو کی حالت صحت مند ہوئی تو آپ کو جواب میں OK لکھا نظر آئے گا۔ بصورت دیگر یہاں آپ کو مسئلے کی نشاندہی کر دی جائے گی۔ یہ بہت مفصل معلومات نہیں۔ اسمارٹ نظام ہارڈ ڈرائیو کے متعلق اس سے کہیں زیادہ ڈیٹا فراہم کرسکتا ہے۔ اس ڈیٹا کو قابل فہم حالت میں دیکھنے کے لئے آپ CrystalDiskInfo نامی یوٹیلیٹی استعمال کرسکتے ہیں۔ یہ سافٹ ویئر درج ذیل ربط سے ڈاؤن لوڈ کیا جاسکتا ہے:

http://crystalmark.info/software/CrystalDiskInfo/index-e.html

یہ یوٹیلیٹی ہارڈ ڈسک سے متعلق مفصل معلومات فراہم کرتی ہے۔ اس کے ذریعے آپ جان سکتے ہیں کہ آیا ہارڈ ڈسک صحت مند ہے یا نہیں۔ اس کا درجہ حرارت کیا ہے اور اہم خصوصیات کی موجودہ صورت حال کیا ہے۔ یہاں کسی بھی گڑبڑ کو دیکھ کر آپ ہارڈ ڈسک کا استعمال جاری رکھنے یا اسے تبدیل کرنے کا فیصلہ کرسکتے ہیں۔ اگر دوران استعمال ہارڈ ڈسک میں کوئی خرابی پیدا ہوتی ہے یا S.M.A.R.T نظام کی حالت میں کوئی تبدیلی واقع ہوتی ہے تو یہ سافٹ ویئر فوراً پاپ اپ کے ذریعے آپ کو اس کے بارے میں بھی مطلع کرتا ہے۔ کرسٹل ڈسک انفو سافٹ ویئر کے علاوہ بھی درجنوں سافٹ ویئر ہارڈ ڈسک کی صحت جانچنے کے لئے استعمال کئے جاسکتے ہیں۔ خاص طور پر Hiren's Bootable CD میں ایسے کئی مفت سافٹ ویئر موجود ہیں۔

سوال: مائیکروسافٹ ایکسل میں زیادہ سے زیادہ کتنی قطاریں اور کتنے کالم بنائے جاسکتے ہیں؟
(جہانگیر خان، فیس بک)

جواب: کسی ایکسل شیٹ میں زیادہ سے زیادہ کتنی قطاریں اور کالم ہوسکتے ہیں، اس بات کا انحصار اس بات پر ہے کہ آپ مائیکروسافٹ آفس/ایکسل کا کون سا ورژن استعمال کررہے ہیں۔ وہ لوگ جو ایکسل کے ایک دہائی سے بھی پرانے ورژن استعمال کررہے ہیں، انہیں اس حوالے سے پریشان ہونے کی شاید ضرورت پیش آتی ہو کیونکہ ایکسل کے ورژن 95 میں زیادہ سے زیادہ 16384 قطاریں اور زیادہ سے زیادہ 256 کالم ہوسکتے یا بنائے جاسکتے ہیں۔ ایکسل کے ورژن 97 میں قطاروں کی تعداد بڑھا کر 65536 کردی گئی تھی لیکن کالم پھر بھی 256 سے زیادہ نہیں بنائے جاسکتے تھے۔ یہ حدیں ایکسل کے ورژن 2003 تک برقرار رہیں۔ پھر مائیکروسافٹ آفس 2007ء میں ان حدوں میں اضافہ کیا گیا۔ ایکسل 2007 سے ایکسل 2013 تک تمام ورژن میں زیادہ سے زیادہ قطاروں کی تعداد دس لاکھ سے بھی زیادہ (1048676) ہوسکتی ہے اور کالم بھی 16384 تک بنائے جاسکتے ہیں۔ یوں ایکسل کے نئے ورژن استعمال کرنے والوں کو عموماً ان حدود کی وجہ سے پریشانی کا سامنا نہیں ہوتا۔ ایسا شاز و نادر ہی ہوتا ہے کہ کسی ایکسل شیٹ میں سولہ ہزار سے زائد کالموں یا دس لاکھ سے زائد قطاروں کو ضرورت پیش آئے۔ اتنے زیادہ ڈیٹا کے لئے ایکسل شاید مناسب سافٹ ویئر بھی نہیں۔

کسی ایکسل اسپریڈ شیٹ یا ورک بک میں ورک شیٹس کی تعداد بھی محدود ہوتی ہے۔ ایکسل 2007 اور 2010 میں زیادہ سے زیادہ 256 ورک شیٹس بنائی یا کھولی جاسکتی ہیں۔ لیکن اس حد کا براہ راست تعلق کمپیوٹر میں دستیاب میموری پر ہے۔ اگر میموری اس قدر نا کافی ہو کہ چار ورک شیٹس بھی نہ کھولی جاسکیں تو 256 ورک شیٹس کی حد غیر موثر ہوسکتی ہے۔ ایکسل کے ورژن 2013 میں ورک شیٹس کی تعداد پر کوئی حد نہیں ہے بلکہ اس کا تعلق کمپیوٹر میں دستیاب RAM پر ہے۔

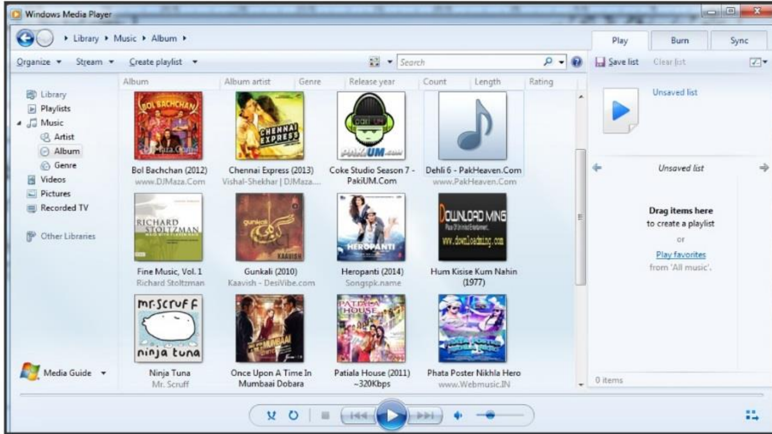
سوال: میں ونڈوز سیون استعمال کررہا ہوں لیکن میرے پاس اپنی ونڈوز سیون کو ونڈوز ٹین پر اپ گریڈ کرنے کے لئے کوئی آئی کن سسٹم ٹرے میں نہیں آرہا۔ میں یہ آئی کن کس طرح بحال کروں؟
(فصیح بخاری، فیس بک)

جواب: جس آئی کن کی بابت آپ نے سوال کیا ہے وہ آئی کن Get Windows 10 app کا ہے۔ مائیکروسافٹ کی ویب سائٹ پر موجود ونڈوز ٹین FAQs کے مطابق اگر آپ کے یہ آئی کن نظر نہیں آرہا ہے تو اس کی درج ذیل وجوہ ہوسکتی ہیں:



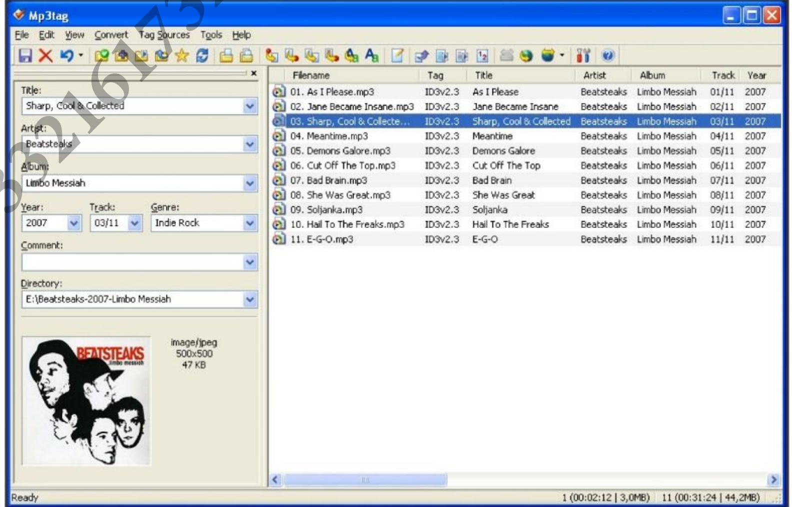
- اگر آپ ونڈوز 7 کا سروس پیک وَن استعمال نہیں کررہے ہے تو یہ آئی کن آپ کو نظر نہیں آئے گا۔ اس لئے آپ پہلے ونڈوز سیون سروس پیک وَن نصب کریں۔
- اگر آپ نے ونڈوز اپ ڈیٹس کو بند کررکھا ہے یا اس کی سروس نہیں چل رہی تو بھی آپ کو یہ آئی کن نظر نہیں آئے گا۔ عموماً غیر قانونی طریقے سے ایکٹی ویٹ کروائی گئی مائیکروسافٹ ونڈوز میں اپ ڈیٹس بھی بند کردی جاتی ہیں تاکہ نئی اپ ڈیٹس ڈاؤن لوڈ نہ ہوں اور ونڈوز کا لائسنس چیک نہ کیا جائے۔ اس کے علاوہ بعض اوقات صارفین خود بھی قانونی ونڈوز رکھنے کے باوجود ونڈوز اپ ڈیٹس کو غیر فعال کردیتے ہیں تاکہ نئی اپ ڈیٹس ڈاؤن لوڈ یا نصب نہ ہوں۔ اس بات کا غالب امکان ہے کہ آپ کے پاس بھی یہی صورت حال ہے۔ اس کے علاوہ یہ بھی ممکن ہے کہ آپ کے پاس ونڈوز اپ ڈیٹ کی سروس تو چل رہی ہو لیکن آپ نے اس خود بخود اپ ڈیٹس ڈاؤن لوڈ کرنے کی اجازت نہ دی ہو۔ اس صورت میں آپ کو خود کنٹرول پینل میں موجود ونڈوز اپ ڈیٹ کے آئی کن پر ڈبل کلک کرکے Check Updates کے بٹن پر کلک کرنا ہوگا۔
- اگر ونڈوز اصلی یا جینوئن نہ ہو تو بھی یہ آئی کن ظاہر نہ ہونے کی ایک وجہ ہوسکتی ہے۔
- اگر آپ کا کمپیوٹر ونڈوز ٹین کو درکار کم سے کم ہارڈ ویئر یا سافٹ ویئر ضروریات پر پورا نہیں اترتا تو بھی آپ کو یہ آئی کن نظر نہیں آئے گا۔
- دفاتر وغیرہ میں استعمال ہونے والے کمپیوٹروں کی اپ ڈیٹس کا انتظام عموماً نیٹ ورک ایڈمنسٹریٹر کے پاس ہوتا ہے۔ اس لئے اگر اس نے Get Windows 10 app کی اپ ڈیٹ کو بند کررکھا ہے تو بھی مذکورہ آئی کن آپ کو سسٹم ٹرے میں دِکھائی نہیں دے گا۔

سوال: ایم پی تھری فائل میں کلپ آرٹ (البم آرٹ) کیسے تبدیل کرتے ہیں؟ یعنی وہ فوٹو جو کسی ایم پی تھری گانے کو میڈیا پلیئر میں چلانے پر ظاہر ہوتی ہے، اسے تبدیل کرنے کا طریقہ بتادیں۔ (سلطان حجبانی، فیس بک)



جواب: پہلے تو یہ بات ذہن نشین کرلیں کہ ہر میوزک البم میں موجود تمام گانوں کا صرف ایک ہی البم آرٹ ہوسکتا ہے۔ یعنی یہ ممکن نہیں کہ آپ ایک البم کے تمام گانوں کا الگ الگ البم آرٹ متعین کرسکیں۔ نیز، اگر آپ مائیکروسافٹ ونڈوز میں پہلے سے موجود ونڈوز میڈیا پلیئر استعمال کررہے ہیں اور انٹرنیٹ سے بھی جڑے ہوئے ہیں، تو ونڈوز میڈیا پلیئر خود ہی گانے سے متعلق البم آرٹ انٹرنیٹ سے تلاش کرکے ظاہر اور محفوظ کرلیتا ہے۔ البم آرٹ تبدیل کرنے کے لئے تھرڈ پارٹی سافٹ ویئر کی ضرورت نہیں۔ اگر آپ ونڈوز 7 یا اس سے نیا ورژن استعمال کررہے ہیں تو البم آرٹ کو ونڈوز میڈیا پلیئر کے ذریعے بھی تبدیل کرسکتے ہیں۔

ونڈوز میڈیا پلیئر کی مدد سے البم آرٹ تبدیل کرنے کے لئے سب سے پہلے ونڈوز میڈیا پلیئر کو کھولیں۔ کی بورڈ سے ALT کا بٹن دبائیں۔ اس سے مینیو ظاہر ہوجائے گا۔ آپ View مینیو میں سے Library پر کلک کریں۔ براہ راست لائبریری کھولنے کے لئے کی بورڈ سے Ctrl اور 1 کا بٹن بیک وقت بھی دبایا جاسکتا ہے۔ اب بائیں طرف موجود فہرست میں سے Music کے تحت موجود Album پر کلک کریں۔ دائیں طرف آپ کو مختلف البم نظر آنا شروع ہوجائیں گی۔ اگر آپ کو اپنے مطلوبہ البم یہاں نظر نہ آرہی ہو تو آپ اسے ماؤس کی مدد سے ڈریگ کرکے یہاں ڈراپ کردیں۔ اب اگلا مرحلہ گانے کے لئے تصاویر کا انتخاب ہے۔ آپ اپنی کوئی ذاتی تصویر یا گوگل امیج سرچ کے ذریعے ڈھونڈی ہوئی کوئی تصویر کاپی کریں (منتخب کرکے کی بورڈ سے Ctrl اور C کا بٹن ایک ساتھ دبائیں)۔ اب ونڈوز میڈیا پلیئر میں واپس آکر اس البم پر ماؤس سے رائٹ کلک کریں اور Paste Album Art پر کلک کریں۔ اس طرح آپ نے جو تصویر کاپی کی تھی، وہ بطور البم آرٹ آپ کی منتخب کردہ البم میں پیسٹ ہوجائے گی۔ البم آرٹ کے لئے تصویر کو چوڑائی اور اونچائی برابر ہونی چاہئے۔ عموماً اس مقصد کے لئے 600x600 پکسلز کی فوٹو استعمال کرنے کی تجویز دی جاتی ہے۔



اگر ونڈوز میڈیا پلیئر کا استعمال آپ کو پسند نہیں یا آپ البم آرٹ کے علاوہ ایم پی تھری فائل کی دیگر معلومات جسے میٹا ڈیٹا کہا جاتا ہے، بھی تبدیل کرنا چاہتے ہیں تو اس مقصد کے لئے آپ MP3Tag نامی مفت سافٹ ویئر استعمال کرسکتے ہیں۔ اس سافٹ ویئر کو درج ذیل ربط سے ڈاؤن لوڈ کیا جاسکتا ہے:

http://www.mp3tag.de/en/download.html

اس سافٹ ویئر کی مدد سے نہ صرف یہ کہ البم آرٹ بلکہ البم کا نام، فائل کا عنوان، اس کا مصنف یا صداکار یا فنکار وغیرہ بھی تبدیل کرسکتے ہیں۔



پاکستان بھر میں کمپیوٹنگ کے ڈسٹری بیوٹرز



شہر	ڈسٹری بیوٹر
کراچی	گلستان نیوز ایجنسی، فریئر مارکیٹ
لاہور	گلزار نیوز ایجنسی، اخبار مارکیٹ
بھکر	عامر نیوز ایجنسی، ریلوے اسٹیشن چوک
رحیم یار خان	چوہدری امانت علی اینڈ سنز
راولپنڈی	اشرف نیوز ایجنسی، کمیٹی چوک، اقبال روڈ
پشاور	زرباغ خان نیوز ایجنٹ، چوک یادگار
حیدرآباد	مہران نیوز ایجنسی
ٹوبہ ٹیک سنگھ	جنگ نیوز ایجنسی، نزد ریلوے کراسنگ، کمالیہ روڈ

✱ **آزاد کشمیر:** اعظم نیوز ایجنسی، میاں محمد روڈ، میر پور

✱ **احمد پور ایسٹ:** اسلامی کتب خانہ، نزد گرلز ہائی اسکول، ڈسٹرکٹ بہاول پور

✱ **احمد پور شرقیہ:** اسلامی کتب خانہ، ضلع بہاولپور

✱ **اوکاڑہ:** رحمت بک اسٹال، نزد ریلوے پل

✱ **بنوں:** امیر جان نیوز ایجنسی، چوک بازار، ضلع بنوں

✱ **بہاولنگر:** دولت خان نیوز ایجنسی، اردو بازار، بہاولنگر

✱ **پنڈی گھیپ:** پاکستان نیوز ایجنسی، مین بازار

✱ **تلہ گنگ:** گلوبل کمپیوٹر سینٹر، اولڈ بس اسٹینڈ، ڈسٹرکٹ چکوال

✱ **تربت:** پاک نیوز ایجنسی، مین روڈ

✱ **جام شورو:** کامریڈ بک سٹال، ریلوے کراسنگ

✱ **جھنگ:** شیخ محمد حسین نیوز ایجنٹ، فوارہ چوک، جھنگ صدر

✱ **جھنگ:** ہمدرد نیوز ایجنسی، رفیقی چوک، شورکوٹ چھاؤنی

✱ **چشتیاں:** شاہین لائبریری، اُردو بازار، ضلع بہاولنگر

✱ **چشتیاں:** دولت خان نیوز ایجنسی، اردو بازار

✱ **چک درہ:** احسان نیوز ایجنسی، چک درہ، ضلع دیر زیریں

✱ **حاصل پور:** محمد وقاص وحید نیوز ایجنسی، ضلع بہاولپور

✱ **خانپور:** چوہدری بشیر امانت علی اینڈ برادرز، ریلوے روڈ

✱ **خانیوال:** طاہر اسٹیشنری مارٹ اینڈ نیوز ایجنسی، کچہری بازار

✱ **ڈسکہ:** فاروق رضا خان، ڈلیکی گورایا

✱ **ڈیرہ اسماعیل خان:** قمر بک اسٹال، اردو بازار

✱ **ڈیرہ غازی خان:** ناصر نیوز ایجنسی، فریدی بازار، ٹریفک چوک

✱ **سرگودھا:** پاکستان اسٹینڈرڈ بک ڈپو، بلاک نمبر 10، پھٹہ منڈی روڈ

✱ **سرگودھا:** پاکستان نیوز ایجنسی، نزد گول چوک، پھٹہ منڈی روڈ

✱ **سکھر:** الفتح نیوز ایجنسی، مہران مرکز

✱ **سیالکوٹ:** علمی مرکز، اردو بازار

✱ **صادق آباد:** چوہدری نیوز ایجنسی، ریلوے روڈ

✱ **کوٹ ادو:** عابد شاپر فروش، بالمقابل بس اسٹینڈ، کوٹ ادو، ضلع مظفر گڑھ

✱ **گجرات:** پاکستان بک سروس، 30، اُردو بازار

✱ **گجرات:** خالد بک ڈپو، مسلم بازار

✱ **گلگت:** نارتھ بکس، مدینہ سپر مارکیٹ

✱ **مظفر گڑھ:** محمد عبداللطیف بلوچ، نیشنل نیوز ایجنسی، قنوان چوک

✱ **میانوالی:** محمدی نیوز ایجنسی، لاری اڈہ

✱ **واہ کینٹ:** خوشبو ڈائجسٹ سینٹر اینڈ لائبریری، نواب آباد

✱ **واہ کینٹ:** حبیب اللہ قمر، میلاد چوک

✱ **وزیر آباد:** نوید نیوز ایجنسی، ریلوے بکسٹال

✱ **ہارون آباد:** خالد مسعود بزمی، بزمی انٹر پرائزز، نزد بلدیہ آفس

اگر کمپیوٹنگ آپ کے علاقے میں دستیاب نہیں تو برائے مہربانی ہمیں اس نمبر پر مطلع فرمائیں

0342-2507857


UHU®
minions
UHU pega pen
UHU stic
UHU® patafix
BOB
STUART
KEVIN
Minions © 2015 Universal Studios. All Rights Reserved.
UHU® – glues anything, anytime.